HALVES OF POINTS OF AN ODD DEGREE HYPERELLIPTIC CURVE IN ITS JACOBIAN

YURI G. ZARHIN

ABSTRACT. Let \( f(x) \) be a degree \((2g+1)\) monic polynomial with coefficients in an algebraically closed field \( K \) with \( \text{char}(K) \neq 2 \) and without repeated roots. Let \( \mathcal{R} \subset K \) be the \((2g+1)\)-element set of roots of \( f(x) \). Let \( C : y^2 = f(x) \) be an odd degree genus \( g \) hyperelliptic curve over \( K \). Let \( J \) be the jacobian of \( C \) and \( J[2] \subset J(K) \) the (sub)group of points of order dividing 2. We identify \( C \) with the image of its canonical embedding \( C \hookrightarrow J \) (the infinite point of \( C \) goes to the identity element of \( J \)). Let \( P = (a, b) \in C(K) \subset J(K) \) and

\[
M_{1/2,P} = \{a \in J(K) \mid 2a = P\} \subset J(K),
\]

which is \( J[2] \)-torsor. In a previous work we established an explicit bijection between the sets \( M_{1/2,P} \) and

\[
\mathcal{R}_{1/2,P} := \{r : \mathcal{R} \to K \mid r(\alpha)^2 = a - \alpha \forall \alpha \in \mathcal{R}; \prod_{\alpha \in \mathcal{R}} r(\alpha) = -b\}.
\]

The aim of this paper is to describe the induced action of \( J[2] \) on \( \mathcal{R}_{1/2,P} \) (i.e., how signs of square roots \( r(\alpha) = \sqrt{a-\alpha} \) should change).

1. INTRODUCTION

Let \( K \) be an algebraically closed field of characteristic different from 2, \( g > 1 \) a positive integer, \( \mathcal{R} \subset K \) a \((2g+1)\)-element set,

\[
f(x) = f_{\mathcal{R}}(x) := \prod_{\alpha \in \mathcal{R}} (x - \alpha)
\]

a degree \((2g+1)\) polynomial with coefficients in \( K \) and without repeated roots, \( C : y^2 = f(x) \) the corresponding genus \( g \) hyperelliptic curve over \( K \) and \( J \) the jacobian of \( C \). We identify \( C \) with the image of its canonical embedding

\[
C \hookrightarrow J, \quad P \mapsto \text{cl}(\{(P) - (\infty)\})
\]

into \( J \) (the infinite point \( \infty \) of \( C \) goes to the identity element of \( J \)). Let \( J[2] \subset J(K) \) be the kernel of multiplication by 2 in \( J(K) \), which is a \( 2g \)-dimensional \( \mathbb{F}_2 \)-vector space. All the \((2g+1)\) points

\[
\mathfrak{M}_\alpha := (\alpha, 0) \in C(K) \subset J(K) \quad (\alpha \in \mathcal{R})
\]

[2010 Mathematics Subject Classification. 14H40, 14G27, 11G10.
Key words and phrases. Hyperelliptic curves, jacobians, Mumford representations.
Partially supported by Simons Foundation Collaboration grant 
\# 585711.
This paper was written during my stay in May-July 2018 at the Max-Planck-Institut für Mathematik (Bonn, Germany), whose hospitality and support are gratefully acknowledged.]
lie in \( J[2] \) and generate it as the \( 2g \)-dimensional \( \mathbb{F}_2 \)-vector space; they satisfy the only relation

\[
\sum_{\alpha \in R} \mathbb{W}_\alpha = 0 \in J[2] \subset J(K).
\]

This leads to a well known canonical isomorphism [3] between \( \mathbb{F}_2 \)-vector spaces \( J[2] \) and \( (\mathbb{F}_2^R)^0 = \{ \phi : R \to \mathbb{F}_2 \mid \sum_{\alpha \in R} \phi(\alpha) = 0 \} \).

Namely, each function \( \phi \in (\mathbb{F}_2^R)^0 \) corresponds to

\[
\sum_{\alpha \in R} \phi(\alpha) \mathbb{W}_\alpha \in J[2].
\]

For example, for each \( \beta \in R \) the point \( W_\beta = \sum_{\alpha \neq \beta} \mathbb{W}_\alpha \) corresponds to the function \( \psi_\beta : R \to \mathbb{F}_2 \) that sends \( \beta \) to 0 and all other elements of \( R \) to 1.

If \( b \in J(K) \) then the finite set

\[
M_{1/2,b} := \{ a \in J(K) \mid 2a = b \} \subset J(K)
\]

consists of \( 2^{2g} \) elements and carries the natural structure of a \( J[2] \)-torsor.

Let \( P = (a, b) \in C(K) \subset J(K) \).

Let us consider, the set

\[
R_{1/2,P} := \{ r : R \to K \mid r(\alpha)^2 = a - \alpha \forall \alpha \in R; \prod_{\alpha \in R} r(\alpha) = -b \}.
\]

Changes of signs in the (even number of) square roots provide \( R_{1/2,P} \) with the natural structure of a \((\mathbb{F}_2^R)^0\)-torsor. Namely, let

\[
\chi : \mathbb{F}_2 \to K^*
\]

be the additive character such that

\[
\chi(0) = 1, \chi(1) = -1.
\]

Then the result of the action of a function \( \phi : R \to \mathbb{F}_2 \) from \( (\mathbb{F}_2^R)^0 \) to \( r : R \to K \) from \( R_{1/2,P} \) is just the product

\[
\chi(\phi) r : R \to K, \quad \alpha \mapsto \chi(\phi(\alpha)) r(\alpha).
\]

On the other hand, I constructed in [8] an explicit bijection of finite sets

\[
R_{1/2,P} \cong M_{1/2,P}, \quad r \mapsto a_r \in M_{1/2,P} \subset J(K).
\]

Identifying (as above) \( J[2] \) and \( (\mathbb{F}_2^R)^0 \), we obtain a second structure of a \((\mathbb{F}_2^R)^0\)-torsor on \( R_{1/2,P} \). Our main result asserts that these two structures actually coincide. In down-to-earth terms this means the following.

**Theorem 1.1.** Let \( r \in R_{1/2,P} \) and \( \beta \in R \). Let us define \( r^\beta \in R_{1/2,P} \) as follows.

\[
r^\beta(\beta) = r(\beta), \quad r^\beta(\alpha) = -r(\alpha) \forall \alpha \in R \setminus \{\beta\}.
\]

Then

\[
a_{r^\beta} = a_r + 2\mathbb{W}_\beta = a_r + \left( \sum_{\alpha \neq \beta} \mathbb{W}_\alpha \right).
\]
Remark 1.2. In the case of elliptic curves (i.e., when \( g = 1 \)) the assertion of Theorem 1.1 was proven in [1, Th. 2.3(iv)].

Example 1.3. If \( P = W_\beta = (\beta, 0) \) then
\[
a_\tau + W_\beta = a_\tau - 2a_\tau = -a_\tau
\]
while
\[
-a_\tau = a_{-\tau}
\]
(see [8, Remark 3.5]). On the other hand, \( r(\beta) = \sqrt{\beta - \beta} = 0 \) for all \( r \) and
\[
r^\beta = r : \alpha \mapsto -r(\alpha) \quad \forall \alpha \in \mathcal{R}.
\]
This implies that
\[
a_\tau^\beta = a_{-\tau} = a_\tau + W_\beta.
\]
This proves Theorem 1.1 in the special case \( P = W_\beta \).

The paper is organized as follows. In Section 2 we recall basic facts about Mumford representations of points of \( J(K) \) and review results of [8], including an explicit description of the bijection between \( \mathcal{R}_{1/2,P} \) and \( \mathcal{M}_{1/2,P} \). In Section 3 we give explicit formulas for the Mumford representation of \( a + W_\beta \) when \( a \) lies neither on the theta divisor of \( J \) nor on its translation by \( W_\beta \), assuming that we know the Mumford representation of \( a \). In Section 4 we prove Theorem 1.1, using auxiliary results from commutative algebra that are proven in Section 5.

2. Halves and square roots

Let \( C \) be the smooth projective model of the smooth affine plane \( K \)-curve
\[
y^2 = f(x) = \prod_{\alpha \in \mathcal{R}} (x - \alpha)
\]
where \( \mathcal{R} \subset \mathbb{A} \) is a \((2g+1)\)-element subset of \( K \). In particular, \( f(x) \) is a monic degree \((2g+1)\) polynomial without repeated roots. It is well known that \( C \) is a genus \( g \) hyperelliptic curve over \( K \) with precisely one infinite point, which we denote by \( \infty \). In other words,
\[
C(K) = \{(a, b) \in K^2 \mid b^2 = \prod_{\alpha \in \mathcal{R}} (a - \alpha)\} \cup \{\infty\}.
\]
Clearly, \( x \) and \( y \) are nonconstant rational functions on \( C \), whose only pole is \( \infty \). More precisely, the polar divisor of \( x \) is \( 2(\infty) \) and the polar divisor of \( y \) is \((2g+1)(\infty)\). The zero divisor of \( y \) is \( \sum_{\alpha \in \mathcal{R}} (\mathcal{M}_\alpha) \). In particular, \( y \) is a local parameter at \( \infty \).

We write \( \iota \) for the hyperelliptic involution
\[
\iota : C \rightarrow C, \quad (x, y) \mapsto (x, -y), \quad \infty \mapsto \infty.
\]
The set of fixed points of \( \iota \) consists of \( \infty \) and all \( \mathcal{M}_\alpha \) \((\alpha \in \mathcal{R})\). It is well known that for each \( P \in C(K) \) the divisor \((P) + \iota(P) - 2(\infty)\) is principal. More precisely, if \( P = (a, b) \in C(K) \) then \((P) + \iota(P) - 2(\infty)\) is the divisor of the rational function \( x - a \) on \( C \). In particular, if \( P = W_\alpha = (\alpha, 0) \) then
\[
2(W_\alpha) - 2(\infty) = \text{div}(x - \alpha).
\]
In particular, \( x - \alpha \) has a double zero at \( \mathcal{M}_\alpha \) (and no other zeros). If \( D \) is a divisor on \( C \) then we write \( \text{supp}(D) \) for its support, which is a finite subset of \( C(K) \).
We write $J$ for the jacobian of $C$, which is a $g$-dimensional abelian variety over $K$. If $D$ is a degree zero divisor on $C$ then we write $\text{cl}(D)$ for its linear equivalence class, which is viewed as an element of $J(K)$. Elements of $J(K)$ may be described in terms of so called Mumford representations (see [3, Sect. 3.12], [7, Sect. 13.2] and Subsection 2.3 below).

We will identify $C$ with its image in $J$ with respect to the canonical regular map $C \hookrightarrow J$ under which $\infty$ goes to the identity element of $J$. In other words, a point $P \in C(K)$ is identified with $\text{cl}((P) - (\infty)) \in J(K)$. Then the action of $\iota$ on $C(K) \subset J(K)$ coincides with multiplication by $-1$ on $J(K)$. In particular, the list of points of order 2 on $C$ consists of all $\mathfrak{M}_\alpha$ ($\alpha \in \mathfrak{A}$).

2.1. Since $K$ is algebraically closed, the commutative group $J(K)$ is divisible. It is well known that for each $b \in J(K)$ there are exactly $2^{2g}$ elements $a \in J(K)$ such that $2a = b$. In [8] we established explicitly the following bijection $\mathfrak{r} \mapsto a_\mathfrak{r}$ between the $2^{2g}$-element sets $\mathfrak{R}_{1/2,p}$ and $M_{1/2,p}$.

If $\mathfrak{r} \in \mathfrak{R}_{1/2,p}$ then for each positive integer $i \leq 2g + 1$ let us consider the $i$th basic symmetric function $s_i(\mathfrak{r}) \in K$ in $(2g + 1)$ elements $\{\mathfrak{r}(\alpha) \mid \alpha \in \mathfrak{A}\}$ (notice that all $\mathfrak{r}(\alpha)$ are distinct, since their squares $\mathfrak{r}(\alpha)^2 = a - \alpha$ are distinct). Let us consider the degree $g$ monic polynomial

$$U_\mathfrak{r}(x) = (-1)^g \left[ (a - x)^g + \sum_{j=1}^{g} s_{2j}(\mathfrak{r})(a - x)^{g-j} \right],$$

and the polynomial

$$V_\mathfrak{r}(x) = \sum_{j=1}^{g} (s_{2j+1}(\mathfrak{r}) - s_1(\mathfrak{r})s_{2j}(\mathfrak{r})) (a - x)^{g-j}$$

whose degree is strictly less than $g$. Let $\{c_1, \ldots, c_g\} \subset K$ be the collection of all $g$ roots of $U_\mathfrak{r}(x)$, i.e.,

$$U_\mathfrak{r}(x) = \prod_{j=1}^{g} (x - c_j) \in K[x].$$

Let us put

$$d_j = V_\mathfrak{r}(c_j) \ \forall j = 1, \ldots, g.$$ 

It is proven in [8, Th. 3.2] that $Q_j = (c_j, d_j)$ lies in $C(K)$ for all $j$ and

$$a_\mathfrak{r} = \text{cl} \left( \sum_{j=1}^{g} (Q_j) \right) - g(\infty) \in J(K)$$

satisfies $2a_\mathfrak{r} = P$, i.e., $a_\mathfrak{r} \in M_{1/2,p}$. In addition, none of $Q_j$ coincides with any $\mathfrak{M}_\alpha$, i.e.,

$$U_\mathfrak{r}(\alpha) \neq 0, \ c_j \neq \alpha, \ d_j \neq 0.$$ 

The main result of [8] asserts that the map

$$\mathfrak{R}_{1/2,p} \rightarrow M_{1/2,p}, \ \mathfrak{r} \mapsto a_\mathfrak{r}$$

is a bijection.
Remark 2.2. Notice that one may express explicitly \( r \) in terms of \( U_t(x) \) and \( V_t(x) \). Namely [8, Th. 3.2], none of \( \alpha \in R \) is a root of \( U_t(x) \) and

\[
v_t(\alpha) = s_1(t) + (-1)^g \frac{V_t(\alpha)}{U_t(\alpha)} \quad \text{for all } \alpha \in R.
\]

In order to determine \( s_1(t) \), let us fix two distinct roots \( \beta, \gamma \in R \). Then [8, Cor. 3.4]

\[
\frac{V_t(\gamma)}{U_t(\gamma)} \neq \frac{V_t(\beta)}{U_t(\beta)}
\]

and

\[
s_1(t) = \frac{(-1)^g}{2} \times \frac{\beta + \left( \frac{V_t(\beta)}{U_t(\beta)} \right)^2 - \left( \gamma + \left( \frac{V_t(\gamma)}{U_t(\gamma)} \right)^2 \right)}{\left( \frac{V_t(\gamma)}{U_t(\gamma)} \right) - \left( \frac{V_t(\beta)}{U_t(\beta)} \right)}.
\]

2.3. Mumford representations (see [3, Sect. 3.12], [7, Sect. 13.2, pp. 411–415, especially, Prop. 13.4, Th. 13.5 and Th. 13.7]). Recall [7, Sect. 13.2, p. 411] that if \( D \) is an effective divisor on \( C \) of (nonnegative) degree \( m \), whose support does not contain \( \infty \), then the degree zero divisor \( D - m(\infty) \) is called semi-reduced if it enjoys the following properties.

- If \( M_\alpha \) lies in \( \text{supp}(D) \) then it appears in \( D \) with multiplicity 1.
- If a point \( Q \) of \( C(\infty) \) lies in \( \text{supp}(D) \) and does not coincide with any of \( M_\alpha \) then \( \nu(Q) \) does not lie in \( \text{supp}(D) \).

If, in addition, \( m \leq g \) then \( D - m(\infty) \) is called reduced.

It is known ([3, Ch. 3a], [7, Sect. 13.2, Prop. 3.6 on p. 413]) that for each \( a \in J(K) \) there exist exactly one nonnegative \( m \) and (effective) degree \( m \) divisor \( D \) such that the degree zero divisor \( D - m(\infty) \) is reduced and \( \text{cl}(D - m(\infty)) = a \). If

\[
m \geq 1, \quad D = \sum_{j=1}^{m} (Q_j) \quad \text{where} \quad Q_j = (a_j, b_j) \in C(K) \quad \text{for all} \quad j = 1, \ldots, m
\]

(here \( Q_j \) do not have to be distinct) then the corresponding

\[
a = \text{cl}(D - m(\infty)) = \sum_{j=1}^{m} Q_j \in J(K).
\]

The Mumford representation of \( a \in J(K) \) is the pair \((U(x), V(x))\) of polynomials \( U(x), V(x) \in K[x] \) such that

\[
U(x) = \prod_{j=1}^{m} (x - a_j)
\]

is a degree \( m \) monic polynomial while \( V(x) \) has degree \(< m = \deg(U) \), the polynomial \( V(x)^2 - f(x) \) is divisible by \( U(x) \), and

\[
b_j = V(a_j), \quad Q_j = (a_j, V(a_j)) \in C(K) \quad \text{for all} \quad j = 1, \ldots, m.
\]

Such a pair always exists, is unique, and (as we have just seen) uniquely determines not only \( a \) but also divisors \( D \) and \( D - m(\infty) \).

Conversely, if \( U(x) \) is a monic polynomial of degree \( m \leq g \) and \( V(x) \) a polynomial such that \( \deg(V) < \deg(U) \) and \( V(x)^2 - f(x) \) is divisible by \( U(x) \) then there exists exactly one \( a = \text{cl}(D - m(\infty)) \) where \( D - m(\infty) \) is a reduced divisor such that \((U(x), V(x))\) is the Mumford representation of \( a = \text{cl}(D - m(\infty)) \).
2.4. In the notation of Subsect. 2.1, let us consider the effective degree \( g \) divisor

\[
D_\varepsilon = \sum_{j=1}^{\infty} (Q_j)
\]

on \( C \). Then \( \text{supp}(D_\varepsilon) \) (obviously) does contain neither \( \infty \) nor any of \( \mathfrak{M}_a \)'s. It is proven in [8] that the divisor \( D_\varepsilon - g(\infty) \) is reduced and the pair \((U_\varepsilon(x), V_\varepsilon(x))\) is the Mumford representation of

\[
a_\varepsilon := \text{cl}(D_\varepsilon - g(\infty)).
\]

In particular, if \( Q \in C(K) \) lies in \( \text{supp}(D) \) (i.e., is one of \( Q_j \)'s) then \( \iota(Q) \) does not.

Lemma 2.5. Let \( D \) be an effective divisor on \( C \) of degree \( m > 0 \) such that \( m \leq 2g+1 \) and \( \text{supp}(D) \) does not contain \( \infty \). Assume that the divisor \( D - m(\infty) \) is principal.

(1) Suppose that \( m \) is odd. Then:

(i) \( m = 2g + 1 \) and there exists exactly one polynomial \( v(x) \in K[x] \) such that the divisor of \( y - v(x) \) coincides with \( D - (2g+1)(\infty) \). In addition, \( \deg(v) \leq g \).

(ii) If \( \mathfrak{M}_a \) lies in \( \text{supp}(D) \) then it appears in \( D \) with multiplicity 1.

(iii) If \( b \) is a nonzero element of \( K \) and \( P = (a,b) \in C(K) \) lies in \( \text{supp}(D) \) then \( \iota(P) = (a, -b) \) does not lie in \( \text{supp}(D) \).

(iv) \( D - (2g + 1)(\infty) \) is semi-reduced (but not reduced).

(2) Suppose that \( m = 2d \) is even. Then:

(i) there exists exactly one monic degree \( d \) polynomial \( u(x) \in K[x] \) such that the divisor of \( u(x) \) coincides with \( D - m(\infty) \);

(ii) every point \( Q \in C(K) \) appears in \( D - m(\infty) \) with the same multiplicity as \( \iota(Q) \);

(iii) every \( W_\alpha \) appears in \( D - m(\infty) \) with even multiplicity.

Proof: All the assertions except (2)(iii) are already proven in [8, Lemma 2.2]. In order to prove the remaining one, let us split the polynomial \( v(x) \) into a product \( v(x) = (x - \alpha)^d v_1(x) \) where \( d \) is a nonnegative integer and \( v_1(x) \in K[x] \) satisfies \( v_1(\alpha) \neq 0 \). Then \( \mathfrak{M}_a \) appears in \( D - m(\infty) \) with multiplicity \( 2d \), because \( (x - \alpha) \) has a double zero at \( \mathfrak{M}_a \). (See also [4].)

Let \( d \leq g \) be a positive integer and \( \Theta_d \subset J \) be the image of the regular map

\[
C^d \to J, \ (Q_1, \ldots, Q_d) \mapsto \sum_{i=1}^{d} Q_i \subset J.
\]

It is well known that \( \Theta_d \) is an irreducible closed \( d \)-dimensional subvariety of \( J \) that coincides with \( C \) for \( d = 1 \) and with \( J \) if \( d = g \); in addition, \( \Theta_d \subset \Theta_{d+1} \) for all \( d < g \). Clearly, each \( \Theta_d \) is stable under multiplication by \(-1\) in \( J \). We write \( \Theta \) for the \((g - 1)\)-dimensional theta divisor \( \Theta_{g-1} \).

Theorem 2.6 (See Th. 2.5 of [8]). Suppose that \( g > 1 \) and let

\[
C_{1/2} := 2^{-1} \bar{C} \subset J
\]

be the preimage of \( C \) with respect to multiplication by \( 2 \) in \( J \). Then the intersection of \( C_{1/2}(K) \) and \( \Theta \) consists of points of order dividing 2 on \( J \). In particular, the intersection of \( C \) and \( C_{1/2} \) consists of \( \infty \) and all \( \mathfrak{M}_a \)'s.
3. Adding Weierstrass points

In this section we discuss how to compute a sum \( a + \mathfrak{M}_\beta \) in \( J(K) \) when \( a \in J(K) \) lies neither on \( \Theta \) nor on its translation \( \Theta + \mathfrak{M}_\beta \). Let \( D - g(\infty) \) be the reduced divisor on \( C \), whose class represents \( a \). Here

\[
D = \sum_{j=1}^{g} (Q_j)
\]

where \( Q_j = (a_j, b_j) \in C(K) \setminus \{\infty\} \)

is a degree \( g \) effective divisor. Let \( (U(x), V(x)) \) be the Mumford representation of \( \text{cl}(D - g(\infty)) \). We have

\[
\deg(U) = g > \deg(V)
\]

\[
U(x) = \prod_{j=1}^{g} (x - a_j), \quad b_j = V(a_j) \forall j
\]

and \( f(x) - V(x)^2 \) is divisible by \( U(x) \).

**Example 3.1.** Assume additionally that none of \( Q_j \) coincides with \( \mathfrak{M}_\beta = (\beta, 0) \), i.e.,

\[ U(\beta) \neq 0. \]

Let us find explicitly the Mumford representation \((U^{[\beta]}(x), V^{[\beta]}(x))\) of the sum

\[
a + \mathfrak{M}_\beta = \text{cl}(D-m(\infty)) + \text{cl}((\mathfrak{M}_\beta)-(\infty)) = \text{cl}((D+(\mathfrak{M}_\beta))-(g+1)(\infty)) = \text{cl}(D_1-(g+1)(\infty)).
\]

where

\[
D_1 := D + \mathfrak{M}_\beta = \left( \sum_{j=1}^{g} (Q_j) \right) + \mathfrak{M}_\beta
\]

is a degree \((g + 1)\) effective divisor on \( C \). (We will see that \( \deg(U^{[\beta]})(x) = g \).) Clearly, \( D_1 - (g + 1)(\infty) \) is semi-reduced but not reduced.

Let us consider the polynomials

\[
U_1(x) = (x - \beta)U(x), \quad V_1(x) = V(x) - \frac{V(\beta)}{U(\beta)} U(x) \in K[x].
\]

Then \( U_1 \) is a degree \((g + 1)\) monic polynomial, \( \deg(V_1) \leq g \),

\[
V_1(\beta) = 0, \quad V_1(a_j) = V(a_j) = b_j \forall j
\]

and \( f(x) - V_1(x)^2 \) is divisible by \( U_1(x) \). (The last assertion follows from the divisibility of both \( f(x) \) and \( V_1(x) \) by \( x - \beta \) combined with the divisibility of \( f(x) - V(x)^2 \) by \( U(x) \).) If we put

\[
a_g + 1 = \beta, \quad b_{g+1} = 0, \quad Q_{g+1} = W_\beta = (\beta, 0)
\]

then

\[
U_1(x) = \prod_{j=1}^{g+1} (x - a_j), \quad D_1 = \sum_{j=1}^{g+1} (Q_j) \quad \text{where} \quad Q_j = (a_j, b_j) \in C(K), \quad b_j = V_1(a_j) \forall j
\]

and \( f(x) - V_1(x)^2 \) is divisible by \( U_1(x) \). In particular, \((U_1(x), V_1(x))\) is the pair of polynomials that corresponds to semi-reduced \( D_1 - (g + 1)(\infty) \) as described in [7, Prop. 13.4 and Th. 3.5]. In order to find the Mumford representation of
cl(D_1 - (g + 1)(\infty)), we use an algorithm described in [7, Th. 13.9]. Namely, let us put
\[ \tilde{U}(x) = \frac{f(x) - V_1(x)^2}{U_1(x)} \in K[x]. \]
Since \( \deg(V_1(x)) \leq g \) and \( \deg(f) = 2g + 1 \), we have
\[ \deg(V_1(x)^2) \leq 2g, \quad \deg(f - V_1(x)^2) = 2g + 1, \quad \deg(\tilde{U}(x)) = g. \]
Since \( f(x) \) is monic, \( f(x) - V_1(x)^2 \) is also monic and therefore \( \tilde{U}(x) \) is also monic, because \( U_1(x) \) is monic. By [7, Th. 13.9], \( U^{[\beta]}(x) = \tilde{U}(x) \) (since the latter is monic and has degree \( g \leq g \)) and \( V^{[\beta]}(x) \) is the remainder of \( -V_1(x) \) with respect to division by \( \tilde{U}(x) \). Let us find this remainder. We have
\[ -V_1(x) = -\left( V(x) - \frac{V(\beta)}{U(\beta)} U(x) \right) = -V(x) + \frac{V(\beta)}{U(\beta)} U(x). \]
Recall that
\[ \deg(V_1) < g = \deg(U) = \deg(\tilde{U}). \]
This implies that the coefficient of \( V_1 \) at \( x^g \) equals \( V(\beta)/U(\beta) \) and therefore
\[ V^{[\beta]}(x) = \left( -V(x) + \frac{V(\beta)}{U(\beta)} U(x) \right) - \frac{V(\beta)}{U(\beta)} \tilde{U}(x) = -V(x) + \frac{V(\beta)}{U(\beta)} \left( U(x) - \tilde{U}(x) \right). \]
Using formulas above for \( U_1, V_1, \tilde{U} \), we obtain that
\[ U^{[\beta]}(x) = \frac{f(x) - \left( V(x) - \frac{V(\beta)}{U(\beta)} U(x) \right)^2}{(x - \beta)\tilde{U}(x)}, \]
\[ V^{[\beta]}(x) = -V(x) + \frac{V(\beta)}{U(\beta)} \left( U(x) - \frac{f(x) - \left( V(x) - \frac{V(\beta)}{U(\beta)} U(x) \right)^2}{(x - \beta)\tilde{U}(x)} \right). \]

**Remark 3.2.** There is an algorithm of David Cantor [7, Sect. 13.3] that explains how to compute the Mumford representation of a sum of arbitrary divisor classes (elements of \( J(K) \)) when their Mumford representations are given.

**Remark 3.3.** Suppose that \( a \in J(K) \) and \( P = 2a \) lies in \( C(K) \) but is not the zero of the group law. Then \( a \) does not lie on the theta divisor (Theorem 2.6) and satisfies the conditions of Example 3.1 for all \( \beta \in \mathfrak{R} \) (see Subsect. 2.1).

### 4. Proof of Main Theorem

Let us choose an order on \( \mathfrak{R} \). This allows us to identify \( \mathfrak{R} \) with \( \{1, \ldots, 2g, 2g+1\} \) and list elements of \( \mathfrak{R} \) as \( \{\alpha_1, \ldots, \alpha_{2g}, \alpha_{2g+1}\} \). Then
\[ f(x) = \prod_{i=1}^{2g+1} (x - \alpha_i) \]
and the affine equation for \( C \setminus \{\infty\} \) is
\[ y^2 = \prod_{i=1}^{2g+1} (x - \alpha_i). \]
Slightly abusing notation, we denote \( \mathfrak{M}_{\alpha_i} \) by \( \mathfrak{M}_i \).
Let us consider the closed affine $K$-subset $\tilde{\mathcal{C}}$ in the affine $K$-space $A^{2g+1}$ with coordinate functions $z_1, \ldots, z_{2g}, z_{2g+1}$ that is cut out by the system of quadratic equations

$$z_1^2 + \alpha_1 = z_2^2 + \alpha_2 = \cdots = z_{2g+1}^2 + \alpha_{2g+1}.$$  

We write $x$ for the regular function $z_1^2 + \alpha_1$ on $\tilde{\mathcal{C}}$, which does not depend on a choice of $i$. By Hilbert’s Nullstellensatz, the $K$-algebra $K[\tilde{\mathcal{C}}]$ of regular functions on $\tilde{\mathcal{C}}$ is canonically isomorphic to the following $K$-algebra. First, we need to consider the quotient $A$ of the polynomial $K[x]$-algebra $K[x][T_1, \ldots, T_{2g+1}]$ by the ideal generated by all quadratic polynomials $T_i^2 - (x - \alpha_i)$. Next, $K[\tilde{\mathcal{C}}]$ is canonically isomorphic to the quotient $A/N(A)$ where $N(A)$ is the nilradical of $A$. In the next section (Example 5.3) we will prove that $A$ has no zero divisors (in particular, $N(A) = \{0\}$) and therefore $\tilde{\mathcal{C}}$ is irreducible. (See also [2].) We write $y$ for the regular function

$$y = -\prod_{i=1}^{2g} z_i \in K[\tilde{\mathcal{C}}].$$

Clearly, $y^2 = \prod_{i=1}^{2g} (x - \alpha_i)$ in $K[\tilde{\mathcal{C}}]$. The pair $(x, y)$ gives rise to the finite regular map of affine $K$-varieties (actually, curves)

$$\mathfrak{h} : \tilde{\mathcal{C}} \to \mathcal{C} \setminus \{\infty\}, \quad (r_1, \ldots, r_{2g}, r_{2g+1}) \mapsto (a, b) = \left(r_1^2 + \alpha_1, -\prod_{i=1}^{2g+1} r_i\right)$$

of degree $2^{2g}$. For each

$$P = (a, b) \in K^2 = A^2(K) \text{ with } b^2 = \prod_{i=1}^{2g+1} (a - \alpha_i)$$

the fiber $\mathfrak{h}^{-1}(P)$ consists of (familiar) collections of square roots $r = \{r_i = \sqrt{a - \alpha_i} \mid 1 \leq i \leq 2g + 1\}$ with $\prod_{i=1}^{2g+1} r_i = -b$. Each such $r$ gives rise to $a_r \in J(K)$ such that

$$2a = P \in \mathcal{C}(K) \subseteq J(K)$$

(see [8, Th. 3.2]). On the other hand, for each $\mathfrak{m}_l = (\alpha_l, 0)$ (with $1 \leq l \leq 2g+1$) the sum $a_r + \mathfrak{m}_l$ is also a half of $P$ and therefore corresponds to the certain collection of square roots. Which one? The answer is given by Theorem 1.1. We repeat its statement, using the new notation.

**Theorem 4.1.** Let $P = (a, b)$ be a $K$-point on $\mathcal{C}$ and $r = (r_1, \ldots, r_{2g}, r_{2g+1})$ be a collection of square roots $r_i = \sqrt{a - \alpha_i} \in K$ such that $\prod_{i=1}^{2g+1} r_i = -b$. Let $l$ be an integer that satisfies $1 \leq l \leq 2g + 1$ and let

$$r^{[l]} = \left(r_1^{[l]}, \ldots, r_{2g}^{[l]}, r_{2g+1}^{[l]}\right) \in \mathfrak{h}^{-1}(P) \subseteq \tilde{\mathcal{C}}(K)$$

be the collection of square roots $r_i^{[l]} = \sqrt{a - \alpha_i}$ such that

$$r_i^{[l]} = r_i, \quad r_i^{[l]} = -r_i \text{ for } \forall i \neq l.$$

Then

$$a_r + \mathfrak{m}_l = a_r^{[l]}.$$
Example 4.2. Let us take as $P$ the point $\mathfrak{M}_l = (\alpha_l, 0)$. Then
\[ r_l = \sqrt{\alpha_l - \alpha_l} = 0 \quad \forall \tau = (r_1, \ldots, r_{2g}, r_{2g+1}) \in \mathfrak{h}^{-1}(\mathfrak{M}_l) \]
and therefore
\[ v^{[l]} = (-r_1, \ldots, -r_{2g}, -r_{2g+1}) = -\tau. \]
It follows from Example 1.3 (if we take $\beta = \alpha_l$) that
\[ a_\tau + \mathfrak{M}_l = a_\tau - W_l = a_\tau - 2a_\tau = -a_\tau = a_{\tau[l]}. \]
This proves Theorem 4.1 in the case of $P = \mathfrak{M}_l$. We are going to deduce the general case from this special one.

4.3. Before starting the proof of Theorem 4.1, let us define for each collections of signs
\[ \varepsilon = \{ \epsilon_i = \pm 1 \mid 1 \leq i \leq 2g + 1, \prod_{i=1}^{2g+1} \epsilon_i = 1 \} \]
the biregular automorphism
\[ T_\varepsilon : \tilde{C} \rightarrow \tilde{C}, \ z_i \mapsto \epsilon_i z_i \ \forall i. \]
Clearly, all $T_\varepsilon$ constitute a finite automorphism group of $\tilde{C}$ that leaves invariant every $K$-fiber of $h : \tilde{C} \rightarrow C \setminus \{\infty\}$, acting on it transitively. Notice that if $T_\varepsilon$ leaves invariant all the points of a certain fiber $h^{-1}(P)$ with $P \in \mathcal{C}(K)$ then all the $\epsilon_i = 1$, i.e., $T_\varepsilon$ is the identity map.

Proof of Theorem 4.1. Let
\[ s^{[l]} : \tilde{C} \rightarrow \tilde{C} \]
be the automorphism (involution) of $\tilde{C}$ defined by (15). We need to define another (actually, it will turn out to be the same) involution (and therefore an automorphism)
\[ t^{[l]} : \tilde{C} \rightarrow \tilde{C} \]
that is defined by
\[ a_{t^{[l]}(\tau)} = a_\tau + \mathfrak{M}_l \]
as a composition of the following regular maps. First, $\tau \in \tilde{C}(K)$ goes to the pair of polynomials $(U_\tau(x), V_\tau(x))$ as in Remark 2.2, which is the Mumford representation of $a_\tau$ (see Subsect. 2.4). Second, $(U_\tau(x), V_\tau(x))$ goes to the pair of polynomials $(U^{[l]}(x), V^{[l]}(x))$ defined in Section 3, which is the Mumford representation of $a_\tau + W_l$. Third, using Remark 2.2 applied to $(U^{[l]}(x), V^{[l]}(x))$, we get at last $t^{[l]}(\tau) \in \mathcal{C}(K)$ such that
\[ a_{t^{[l]}(\tau)} = a_\tau + W_l. \]
Clearly, $t^{[l]}$ is a regular map of $\tilde{C}$ into itself that is an involution, which implies that $t^{[l]}$ is a biregular automorphism of $\tilde{C}$. It is also clear that both $s^{[l]}$ and $t^{[l]}$ leave invariant every fiber of $h : \tilde{C} \rightarrow C \setminus \{\infty\}$ and coincide on $h^{-1}(\mathfrak{M}_l)$, thanks to Example 4.2. This implies that $u := (s^{[l]})^{-1} t^{[l]}$ is a biregular automorphism of $\tilde{C}$ that leaves invariant every fiber of $h : \tilde{C} \rightarrow C \setminus \{\infty\}$ and acts as the identity map on $h^{-1}(\mathfrak{M}_l)$. The invariance of each fiber of $h$ implies that $\mathcal{C}(K)$ coincides with the finite union of its closed subsets $\mathcal{C}_\varepsilon$ defined by the condition
\[ \tilde{C}_\varepsilon := \{ Q \in \tilde{C}(K) \mid u(Q) = T_\varepsilon(Q) \}. \]
Since \( \tilde{C} \) is irreducible, the whole \( \tilde{C}(K) \) coincides with one of \( \tilde{C}_z \). In particular, the fiber
\[
\mathfrak{h}^{-1}(\mathfrak{M}_l) \subset \tilde{C}_z
\]
and therefore \( T_z \) acts identically on all points of \( \mathfrak{h}^{-1}(\mathfrak{M}_l) \). In light of arguments of Subsect. 4.3, \( T_z \) is the identity map and therefore \( u \) acts identically on the whole \( \tilde{C}(K) \). This means that \( s^{[l]} = t^{[l]} \), i.e.,
\[
a_t + \mathfrak{M}_l = a_t^{[l]}.
\]

4.4. Let \( \phi : \mathcal{R} \rightarrow \mathbb{F}_2 \) be a function that satisfies \( \sum_{\alpha \in \mathcal{R}} \phi(\alpha) = 0 \), i.e. \( \phi \in (\mathbb{F}_2^{\mathcal{R}})^0 \). Then the finite subset
\[
\text{supp}(\phi) = \{ \alpha \in \mathcal{R} \mid \phi(\alpha) \neq 0 \} \subset \mathcal{R}
\]
has even cardinality and the correspondent point of \( J[2] \) is
\[
\mathfrak{T}_\phi = \sum_{\alpha \in \mathcal{R}} \phi(\alpha) \mathfrak{M}_\alpha = \sum_{\alpha \in \text{supp}(\phi)} \mathfrak{M}_\alpha = \sum_{\gamma \notin \text{supp}(\phi)} \mathfrak{M}_\gamma.
\]

**Theorem 4.5.** Let \( r \in \mathcal{R}_{1/2,P} \). Let us define \( r^{(\phi)} \in \mathcal{R}_{1/2,P} \) as follows.
\[
r^{(\phi)}(\alpha) = -r(\alpha) \forall \alpha \in \text{supp}(\phi); \quad r^{(\phi)}(\gamma) = r(\gamma) \forall \gamma \notin \text{supp}(\phi).
\]
Then
\[
a_t + \mathfrak{T}_\phi = a_t^{(\phi)}.
\]

**Remark 4.6.** If \( \phi \) is identically zero then
\[
\mathfrak{T}_\phi = 0 \in J[2], \quad r^{(\phi)} = r
\]
and the assertion of Theorem 4.5 is obviously true. If \( l \in \mathcal{R} \) and \( \phi = \psi_l \), i.e. \( \text{supp}(\phi) = \mathcal{R} \setminus \{ l \} \) then
\[
\mathfrak{T}_\phi = \mathfrak{M}_l \in J[2] \quad r^{(\phi)} = r^{[l]}
\]
and the assertion of Theorem 4.5 follows from Theorem 4.1.

**Proof of Theorem 4.5.** We may assume that \( \phi \) is not identically zero. We need to apply Theorem 4.1 \( d \) times where \( d \) is the (even) cardinality of \( \text{supp}(\phi) \) in order to get \( r' \in \mathcal{R}_{1/2,P} \) such that
\[
a_t + \sum_{\alpha \in \text{supp}(\phi)} \mathfrak{M}_\alpha = a_t^{r'}.
\]
Let us check how many times do we need to change the sign of each \( r(\beta) \). First, if \( \beta \notin \text{supp}(\phi) \) then we need to change to sign of \( r(\beta) \) at every step, i.e., we do it exactly \( d \) times. Since \( d \) is even, the sign of \( r(\beta) \) remains the same, i.e.,
\[
r'(\beta) = r(\beta) \forall \beta \notin \text{supp}(\phi).
\]
Now if \( \beta \in \text{supp}(\phi) \) then we need to change the sign of \( r(\beta) \) every time when we add \( W_\alpha \) with \( \alpha \neq \beta \) and it occurs exactly \((d - 1)\) times. On the other hand, when we add \( \mathfrak{M}_\beta \), we don’t change the sign of \( r(\beta) \). So, we change the sign of \( r(\beta) \) exactly \((d - 1)\) times, which implies that
\[
r'(\beta) = -r(\beta) \forall \beta \in \text{supp}(\phi).
\]
Combining the last two displayed formula, we obtained that
\[
r' = r^{(\phi)}.
\]
5. Useful Lemma

The following result is probably well known but I did not find a suitable reference. (However, see [2, Lemma 5.10].)

Lemma 5.1. Let $n$ be a positive integer, $E$ a field provided with $n$ distinct discrete valuation maps

$$\nu_i : E^* \to \mathbb{Z}, \ (i = 1, \ldots, n).$$

For each $i$ let $O_{\nu_i} \subset E$ the discrete valuation ring attached to $\nu_i$ and $\pi_i \in O_{\nu_i}$ its uniformizer, i.e., a generator of the maximal ideal in $O_{\nu_i}$. Suppose that for each $i$ we are given a prime number $p_i$ such that the characteristic of the residue field $O_{\nu_i}/\pi_i$ is different from $p_i$ for all $k \neq i$. Let us assume also that

$$\nu_i(\pi_k) = \delta_{ik} \ \forall i, k = 1, \ldots, n,$$

i.e., each $\pi_i$ is a $\nu_k$-adic unit if $i \neq k$.

Then the quotient $B = E[T_1, \ldots, T_n]/(T_i^{p_i} - \pi_1, \ldots, T_n^{p_n} - \pi_n)$ of the polynomial $E$-algebra $E[T_1, \ldots, T_n]$ by the ideal generated by all $T_i^{p_i} - \pi_i$ is a field that is an algebraic extension of $E$ of degree $\prod_{i=1}^n p_i$. In addition, the set of monomials

$$S = \{ \prod_{i=1}^n T_i^{e_i} \mid 0 \leq e_i \leq p_i - 1 \} \subset E[T_1, \ldots, T_n]$$

maps injectively into $B$ and its image is a basis of the $E$-vector space $B$.

Proof. First, the cardinality of $S$ is $\prod_{i=1}^n p_i$ and the image of $S$ generates $B$ as the $E$-vector space. This implies that if the $E$-dimension of $B$ is $\prod_{i=1}^n p_i$ then the image of $S$ is a basis of the $E$-vector space $B$. Second, notice that for each $i$ the polynomial $T_i^{p_i} - \pi_i$ is irreducible over $E$, thanks to the Eisenstein criterion applied to $\nu_i$ and therefore $E[T_i]/(T_i^{p_i} - \pi_i)$ is a field that is an algebraic degree $p_i$ extension of $E$. In particular, the $E$-dimension of $E[T_i]/(T_i^{p_i} - \pi_i)$ is $p_i$. This proves Lemma for $n = 1$.

Induction by $n$. Suppose that $n > 1$ and consider the finite degree $p_i$ field extension $E_n = E[T_n]/(T_n^{p_n} - \pi_n)$ of $E$.

Clearly, the $E$-algebra $B$ is isomorphic to the quotient $E_n[T_1, \ldots, T_{n-1}]/(T_1^{p_1} - \pi_1, \ldots, T_{n-1}^{p_{n-1}} - \pi_{n-1})$ of the polynomial ring $E_n[T_1, \ldots, T_{n-1}]$ by the ideal generated by all polynomials $T_i^{p_i} - \pi_i$ with $i < n$. Our goal is to apply the induction assumption to $E_n$ instead of $E$. In order to do that, let us consider for each $i < n$ the integral closure $\tilde{O}_i$ of $O_{\nu_i}$ in $E_n$. It is well known that $\tilde{O}_i$ is a Dedekind ring. Our conditions imply that $E_n/E$ is unramified at all $\nu_i$ for all $i < n$. This means that if $\mathcal{P}_i$ is a maximal ideal of $\tilde{O}_i$ that contains $\pi_i\tilde{O}_i$ (such an ideal always exists) and

$$\text{ord}_{\mathcal{P}_i} : E_n^* \to \mathbb{Z}$$

is the discrete valuation map attached to $\mathcal{P}_i$ then the restriction of $\text{ord}_{\mathcal{P}_i}$ to $E^*$ coincides with $\nu_i$. This implies that for all positive integers $i, k \leq n - 1$

$$\text{ord}_{\mathcal{P}_i}(\pi_k) = \nu_i(\pi_k) = \delta_{ik}.$$

In particular,

$$\text{ord}_{\mathcal{P}_i}(\pi_i) = \nu_i(\pi_i) = 1,$$
i.e., $\pi_i$ is a uniformizer in the corresponding discrete valuation (sub)ring $O_{\text{ord} \pi_i}$ of $E_n$ attached to $\text{ord} \pi_i$. Now the induction assumption applied to $E_n$ and its $(n-1)$ discrete valuation maps $\text{ord} \pi_i$ ($1 \leq i \leq n-1$) implies that $B/E_n$ is a field extension of degree $\prod_{i=1}^{n-1} p_i$. This implies that the degree
\[ [B : E] = [B : E_n][E_n : E] = \left( \prod_{i=1}^{n-1} p_i \right) p_n = \prod_{i=1}^{n} p_i. \]
This means that the $E$-dimension of $B$ is $\prod_{i=1}^{n} p_i$ and therefore the image of $S$ is a basis of the $E$-vector space $B$. \square

**Corollary 5.2.** We keep the notation and assumptions of Lemma 5.1. Let $R$ be a subring of $E$ that contains 1 and all $\pi_i$ ($1 \leq i \leq n$). Then the quotient $B_R = R[T_1, \ldots, T_n]/(T_1^{p_1} - \pi_1, \ldots, T_n^{p_n} - \pi_n)$ of the polynomial $R$-algebra $R[T_1, \ldots, T_n]$ by the ideal generated by all $T_i^{p_i} - \pi_i$ has no zero divisors.

**Proof.** There are the natural homomorphisms of $R$-algebra
\[ R[T_1, \ldots, T_n] \to B_R \to B \]
such that the first homomorphism is surjective and the injective image of
\[ S \subset R[T_1, \ldots, T_n] \subset E[T_1, \ldots, T_n] \]
in $B$ is a basis of the $E$-vector space $B$. On the other hand, the image of $S$ generates $B_R$ as $R$-module. It suffices to prove that $B_R \to B$ is injective, since $B$ is a field by Lemma 5.1.

Suppose that $u \in B_R$ goes to 0 in $B$ is zero. Recall that $u$ is a linear combination of (the images of) elements of $S$ with coefficients in $R$. Since the image of $u$ in $B$ is 0, all these coefficients are zeros, i.e., $u = 0$ in $B_R$. \square

**Example 5.3.** We use the notation of Section 4. Let us put $n = 2g + 1$, $R = K[x], E = K(x), \pi_i = x - \alpha_i, p_i = 2$ and let
\[ \nu_i : E^* = K(x)^* \to \mathbb{Z} \]
be the discrete valuation map of the field of rational functions $K(x)$ attached to $\alpha_i$. Then $K[\tilde{C}] = B_R/\mathcal{N}(B_R)$ where $\mathcal{N}(B_R)$ is the nilradical of $B_R$. It follows from Corollary 5.2 that $\mathcal{N}(B_R) = \{0\}$ and $K[\tilde{C}]$ has no zero divisors, i.e., $\tilde{C}$ is irreducible.

**References**

[1] B.M. Bekker, Yu.G. Zarhin, *The divisibility by 2 of rational points on elliptic curves*. Algebra i Analiz 29:4 (2017), 196–239; St. Petersburg Math. J. 29 (2018), 683–713.

[2] N. Bruin and E.V. Flynn, *Towers of 2-covers of hyperelliptic curves*. Trans. Amer. Math. Soc. 357 (2005), no. 11, 4329–4347.

[3] D. Mumford, Tata Lectures on Theta. II. Progress in Math. 43, Birkhäuser, Boston Basel Stuttgart, 1984.

[4] M. Stoll, *Arithmetic of Hyperelliptic Curves*. Available at Summer Semester 2014, University of Bayreuth. http://www.mathe2.uni-bayreuth.de/stoll/teaching/ArithHypKurvenSS2014/Skript-ArithHypCurves-pub-screen.pdf.

[5] E. Schaefer, 2-descent on the Jacobians of hyperelliptic curves. J. Number Theory 51 (1995), no. 2, 219–232.

[6] J.-P. Serre, *Algebraic groups and class fields*. Graduate Texts in Math. 117, Springer-Verlag, New York, 1988.

[7] L.C. Washington, *Elliptic Curves: Number Theory and Cryptography*. Second edition. Chapman & Hall/CRC Press, Boca Raton London New York, 2008.
[8] Yu. G. Zarhin, *Division by 2 on odd degree hyperelliptic curves and their jacobians*. MPIM (Bonn) Preprint Series, 2018 (31); available at https://www.mpim-bonn.mpg.de/preblob/5876 .

Pennsylvania State University, Department of Mathematics, University Park, PA 16802, USA

E-mail address: zarhin@math.psu.edu