manuscripta math. 120, 403–413 (2006)

V. G. Lopez Neumann · Constantin Manoil

Rational classes and divisors on curves of genus 2

Received: 1 May 2005
Published online: 1 July 2006

Abstract. We describe a method of looking for rational divisor classes on a curve of genus 2. We have an algorithm to decide if a given class of divisors of degree 3 contains a rational divisor. It is known that the shape of the kernel of Cassel's morphism $(X - T)$ is related to the existence of rational classes of degree 1. Our key tool is the dual Kummer surface.

1. Introduction

We draw the attention of the reader on the fact that every comment or reference concerning the Brauer–Manin obstruction is made under the assumption that the Tate-Shafarevich group is finite.

There are several reasons to look for rational divisor classes of degree 3 and rational divisors in such classes, on a curve of genus 2. Note that adding an appropriate integer multiple of the canonical class one obtains a bijection between rational classes of any odd degree.

If $\left(\mathrm{Pic}^1\overline{\mathcal{C}}\right)^G = \emptyset$ (see Sect. 2 for notations and definitions), the Brauer–Manin obstruction is the only obstruction to the Hasse principle for a smooth proper curve defined over a number field k (see [9], Corollary 6.2.5).

Also, a main tool for computing the Mordell–Weil group is the homomorphism

$$\Phi = (X - T) : \mathfrak{G} \longrightarrow \mathcal{L} = L^*/k^*(L^*)^2 \quad \text{where } L = k[T]/(F(T)),$$

as defined in [3]. Its kernel is related to rational classes of degree 1, as shown in [6]. In Sect. 4 of this paper we give a method for searching for rational divisor classes of degree 3.

Finally, for curves of genus 2, to decide whether any rational class contains a rational divisor (the so called BigPic property) only divisor classes of degree 3 matter and BigPic holds iff in *a given* rational class there is a rational divisor (see [4], Sect. 3). Section 3 of this paper gives a method for solving this problem.

V. G. L. Neumann supported by CNPq, Brazil

V. G. L. Neumann: UFMG, Belo Horizonte, Brazil. e-mail: gonzalo@mat.ufmg.br

C. Manoil (✉): University of Geneva, CP 64, 1211 Geneva 4, Switzerland.
e-mail: constantin.manoil@math.unige.ch

Mathematics Subject Classification (2000): 11G30 · 14J28 · 11G10

DOI: 10.1007/s00229-006-0021-y

2. Background and notations

Let k be a perfect field of characteristic different from 2 and $G = \mathrm{Gal}\,(\bar{k}/k)$.

Definition 2.1. *Let X be a proper, geometrically integral variety, defined over k. We denote by* $\mathrm{Pic}\, X$ *the divisor classes containing a divisor defined over k and by* $(\mathrm{Pic}\,\overline{X})^G$ *the classes invariant under the action of G. There is an injection*

$$\mathrm{Pic}\, X \longrightarrow \left(\mathrm{Pic}\,\overline{X}\right)^G$$

The property BigPic is defined by

$$\mathrm{BP}\,(X,k) \Leftrightarrow \mathrm{Pic}\, X = (\mathrm{Pic}\,\overline{X})^G.$$

By curve we mean a projective irreducible smooth curve. The linear equivalence class of a divisor $\mathcal{U}$ on the curve $\mathcal{C}$ is denoted by $[\mathcal{U}]$. We denote by $\mathcal{J} = \mathrm{Pic}^0\overline{\mathcal{C}}$ the Jacobian of $\mathcal{C}$ and $\mathfrak{G} = \mathcal{J}(k) = \left(\mathrm{Pic}^0\overline{\mathcal{C}}\right)^G$ the Mordell–Weil group. For genus 2 curves this is the same as $\mathrm{Pic}^0\mathcal{C}$ (see [4], Lemmas 3.1 and 3.2). Every curve defined over k of genus 2 is birationally equivalent over k to a plane sextic

$$\mathcal{C}:\ Y^2 = F(X) = f_0 + f_1X + \cdots + f_6X^6 \in k[X]$$

where F has no multiple factors. The points with $\frac{1}{X} = 0$, $\frac{Y}{X^3} = \pm\sqrt{f_6}$ on the completion of $\mathcal{C}$ are called the points at infinity. For any point $P = (x, y)$, we denote by $\overline{P} = (x, -y)$ the conjugate of P under the $\pm Y$ involution and extend this notation and terminology to divisors.

Let $P_1, P_2 \in \mathcal{C}(\bar{k})$; we denote by $K_{\mathcal{C}}$ a divisor in the canonical class and by $\{P_1, P_2\} \in \mathcal{J}(\bar{k})$ the class of the divisor $P_1 + P_2 - K_{\mathcal{C}}$.

3. Rational divisors

Starting from a curve of genus 2 one can construct the Kummer surface and its dual. These are quartics in $\mathbb{P}^3$. The Kummer $\mathcal{K}$ (respectively its dual $\mathcal{K}^*$) classifies divisors of degree 2 (respectively of degree 3) up to linear equivalence and $\pm Y$ involution. The rational points of $\mathcal{K}^*$ correspond to elements of $\mathrm{Pic}^3\overline{\mathcal{C}}$ defined over k or defined over a quadratic extension and whose Galois conjugates are the conjugates under $\pm Y$ involution. We look for rational points on $\mathcal{K}^*$. When such a point is found, we are able to decide if the corresponding divisor class is rational and if it contains a rational divisor (Proposition 3.5). We can compute a rational divisor in any class which contains one (cf. Proposition 3.5 and Examples 4.2 and 4.3). Our method is different from that proposed by Bruin and Flynn (see [1]).

We give the construction of $\mathcal{K}^*$ in [2], Chapter 4. This can be generalized to divisors of degree $g + 1$, in general position, on a hyperelliptic curve of genus g. The main result is that the corresponding variety is still birational to the Kummer variety; this is work in progress, which will be submitted for publication under the title "A Generalization of the Dual Kummer Surface".

Definition 3.1. *An effective divisor $\mathcal{U}$ on $\mathcal{C}$ of degree* 3 *is in general position if it is given by*

$$U(X) = 0, \quad Y = W(X),$$

where U, $W \in \bar{k}[X]$ have degree at most 3*, such that there exists a polynomial $V \in \bar{k}[X]$ for which*

$$F = W^2 - UV.$$

If U has degree less than 3*, then some of the points of the support of $\mathcal{U}$ are at infinity.*

It is easy to see that divisors in general position are exactly those not equivalent to $P + K_{\mathcal{C}}$ with $P \in \mathcal{C}(\bar{k})$.

The following lemma can be stated and proven in a more general and conceptual form; see

http://arxiv.org/abs/math.AG/0604545

Lemma 3.2. *The linear equivalence classes of effective divisors of degree* 3 *in general position are in* 1 *to* 1 *correspondence with proper equivalence classes of representations of F by $W^2 - UV$, where U, V, W have degree at most* 3*. The involution $Y \mapsto -Y$ corresponds to $U \mapsto U$, $V \mapsto V$, $W \mapsto -W$. Hence an improper automorphism of $W^2 - UV$ (i.e. of determinant -1) takes the corresponding element of* $\mathrm{Pic}^3\overline{\mathcal{C}}$ *into its conjugate.*

Remark 3.3. Let Ω be the matrix

$$\Omega = \begin{pmatrix} 0 & -\frac{1}{2} & 0 \\ -\frac{1}{2} & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

An automorphism of $W^2 - UV$ has a matrix A acting on the column vector (U, V, W) by multiplication on the left such that $A^t \Omega A = \Omega$. The automorphism is proper if $\det A = 1$, it is improper if $\det A = -1$.

One introduces new variables x_0, x_1, x_2, x_3 which establish a linear correspondence between linear forms $u(x_0, \ldots, x_3)$ and polynomials $U(X)$ of degree at most 3 given by

$$x_j \overset{\psi}{\longmapsto} X^j \quad \text{for } 0 \le j \le 3\,. \tag{1}$$

The quadratic form

$$S = S(x_0, x_1, x_2, x_3) = w^2 - uv \tag{2}$$

is unchanged under automorphisms of $W^2 - UV$, so by Lemma 3.2 the form S depends only on the element $[\mathcal{U}] \in \mathrm{Pic}^3\overline{\mathcal{C}}$. In fact $[\mathcal{U}]$ and $[\overline{\mathcal{U}}]$ give the same quadratic form. The quadratic form S is defined over k iff $[\mathcal{U}] \in \left(\mathrm{Pic}^3\overline{\mathcal{C}}/\pm Y\right)^G$.

The form

$$S_4 = f_0x_0^2 + f_1x_0x_1 + f_2x_1^2 + f_3x_1x_2 + f_4x_2^2 + f_5x_2x_3 + f_6x_3^2$$

corresponds to F under ψ. A basis of the kernel of ψ acting on the space of quadratic forms is

$$\begin{aligned} S_1 &= x_0x_2 - x_1^2, \\ S_2 &= x_0x_3 - x_1x_2, \\ S_3 &= x_1x_3 - x_2^2. \end{aligned}$$

Denote by u_j the coefficient of X^j in U, etc. The equation $F = W^2 - UV$ is equivalent to

$$S = w^2 - uv = \sum_1^4 \eta_j S_j, \tag{3}$$

where

$$\begin{aligned} \eta_1 &= 2w_0w_2 - u_0v_2 - u_2v_0, \\ \eta_2 &= 2w_0w_3 - u_0v_3 - u_3v_0, \\ \eta_3 &= 2w_1w_3 - u_1v_3 - u_3v_1, \\ \eta_4 &= 1. \end{aligned}$$

The symmetric matrix of the singular form (3) is

$$Q = \frac{1}{2}\begin{pmatrix} 2f_0\eta_4 & f_1\eta_4 & \eta_1 & \eta_2 \\ f_1\eta_4 & 2f_2\eta_4 - 2\eta_1 & f_3\eta_4 - \eta_2 & \eta_3 \\ \eta_1 & f_3\eta_4 - \eta_2 & 2f_4\eta_4 - 2\eta_3 & f_5\eta_4 \\ \eta_2 & \eta_3 & f_5\eta_4 & 2f_6\eta_4 \end{pmatrix}.$$

Definition 3.4. *The dual Kummer surface is the singular quartic $\mathcal{K}^* \subset \mathbb{P}^3$ given by the equation $det(Q) = 0$ in the variables η_j.*

For a point η on $\mathcal{K}^*$ with $\eta_4 \neq 0$, we take $\eta_4 = 1$ by homogeneity. The quadratic form $S = \sum \eta_j S_j$ is singular and of rank at least 2 (since $\psi(S) = F$ and F has no multiple factors) and thus representable over $\bar{k}$ as $w^2 - uv$. The transformation (1) gives polynomials $U(X)$, $V(X)$, $W(X)$ defining an effective divisor $\mathcal{U}$ of degree 3 on $\mathcal{C}$. The point η determines completely the class of $\mathcal{U}$ up to linear equivalence and $\pm Y$ involution. If $\eta \in \mathcal{K}^*(k)$ the class $[\mathcal{U}]$ is defined over k or over a quadratic extension $k \subset k'$ and in this case $[\mathcal{U}]^\sigma = [\overline{\mathcal{U}}]$ for the non-trivial $\sigma \in \mathrm{Gal}\,(k'/k)$.

By a specialization argument, the points of $\mathcal{K}^*$ with $\eta_4 = 0$ correspond to classes of divisors not in general position :

$$[(x, y) + K_{\mathcal{C}}] \mapsto (x^2, -x, 1, 0).$$

where $x = \eta_2/\eta_3$. If $\eta_3 = 0$, the point (x, y) is at infinity. The rationality of this divisor amounts to that of y.

Now, let $\eta \in \mathcal{K}^*(k)$ be a point with $\eta_4 = 1$ and S the corresponding quadratic form. Since $S = w^2 - uv$, its rank is 3 iff the forms u, v and w are linearly independent and else is 2. Bringing S to diagonal form over k, one obtains a form $a_1{y_1}^2 + a_2{y_2}^2 + a_3{y_3}^2$ of rank 2 or 3. Our goal is to determine when the corresponding divisor class is rational and if this is the case, if there exists a rational divisor in this class.

Proposition 3.5. *Let $\eta \in \mathcal{K}^*(k)$ be a point with $\eta_4 = 1$, let S be the quadratic form obtained from the Eq. (3) and $a_1{y_1}^2 + a_2{y_2}^2 + a_3{y_3}^2$ its diagonal form, where $a_1, a_2, a_3 \in k$ and y_1, y_2, y_3 are k-linear forms in (x_0, x_1, x_2, x_3).*

Let α, β be the square roots of a_3 and $-a_2/a_1$ respectively and let $\mathcal{U}$ be the divisor given by $U(X) = 0$ and $Y = W(X)$, where

$$\begin{aligned} u &= -a_1(y_1 - \beta y_2), \\ v &= y_1 + \beta y_2, \\ w &= \alpha y_3, \end{aligned} \qquad \text{and} \qquad \begin{pmatrix} U \\ V \\ W \end{pmatrix} = \psi \begin{pmatrix} u \\ v \\ w \end{pmatrix}.$$

(i) rank $S = 3$*: The class $[\mathcal{U}]$ is rational iff $-a_1a_2a_3$ is a square in k. If so, $[\mathcal{U}]$ contains a rational divisor iff $a_1{y_1}^2 + a_2{y_2}^2 + a_3{y_3}^2$ represents 0 over k.*

(ii) rank $S = 2$*, ($a_3 = 0$): The class $[\mathcal{U}]$ is always rational and it contains a rational divisor iff the form $a_1{y_1}^2 + a_2{y_2}^2 - y^2$ represents 0 over k.*

Proof. For any $\sigma \in G$, there exists an automorphism of matrix A of $w^2 - uv$, such that $t^\sigma = At$, where $t = \begin{pmatrix} u \\ v \\ w \end{pmatrix}$ and the matrix A is one of the matrices I, B, C or BC, where:

$$B = \underbrace{\begin{pmatrix} 0 & -a_1 & 0 \\ -\frac{1}{a_1} & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}}_{\text{proper}} \quad \text{and} \quad C = \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}}_{\text{improper}}.$$

Recall that $\mathcal{U}^\sigma \sim \mathcal{U}$ if A is proper and $\mathcal{U}^\sigma \sim \overline{\mathcal{U}}$ else. In the case of rank $S = 3$, we have:

$$\begin{gathered} \forall \sigma \in G \text{ we have } \mathcal{U}^\sigma \sim \mathcal{U} \\ \Longleftrightarrow \\ \forall \sigma \in G \text{ we have } t^\sigma = t \text{ or } t^\sigma = Bt \\ \Longleftrightarrow \\ \alpha^\sigma \beta^\sigma = \alpha\beta, \ \forall \sigma \in G \\ \Longleftrightarrow \\ \alpha\beta \in k \\ \Longleftrightarrow \\ -a_1a_2a_3 \text{ is a square in } k. \end{gathered}$$

For rank $S = 2$, we have $\alpha = 0$ and $t^\sigma = t$ or $t^\sigma = Bt$ for any $\sigma \in G$; thus $\mathcal{U} \sim \mathcal{U}^\sigma \sim \overline{\mathcal{U}}$. The first part of the statement is proved for both cases. Now we come to rational divisors.

(i) In rank three, suppose that $[\mathcal{U}]$ contains a rational divisor given by

$$U_1(X) = 0,\ Y = W_1(X) \quad \text{with} \quad \psi \begin{pmatrix} u' \\ v' \\ w' \end{pmatrix} = \begin{pmatrix} U_1 \\ V_1 \\ W_1 \end{pmatrix},$$

where u', v', w' are k-linear forms. Then $a_1 {y_1}^2 + a_2 {y_2}^2 + a_3 {y_3}^2$ is equivalent over k to ${w'}^2 - u'v'$, which obviously represents 0 over k.
Conversely, if $a_1 {y_1}^2 + a_2 {y_2}^2 + a_3 {y_3}^2$ represents 0 over k, there exist rational linear forms u', v', w' such that $S = u'v' + \delta {w'}^2 = \left(\sqrt{\delta} w'\right)^2 - u'(-v')$. This is equivalent over k to ${w^\star}^2 - u^\star v^\star$ iff $\delta \in (k^*)^2$. But

$$a_1 a_2 a_3 = \text{disc}\,(a_1 {y_1}^2 + a_2 {y_2}^2 + a_3 {y_3}^2) = \gamma^2 \text{disc}\,(u'v' + \delta {w'}^2) = -\gamma^2 \delta / 4$$

for some $\gamma \in k^*$, so δ is a square iff $-a_1 a_2 a_3$ is. Since $[\mathcal{U}]$ is rational, $-a_1 a_2 a_3$ is a square by the first part of the proof, so $\delta \in k^*$.

(ii) For rank two, suppose that

$$S = {w'}^2 - u'v' = a_1 y_1^2 + a_2 y_2^2$$

where u', v', w' are linearly dependent k-linear forms in y_1, y_2, y_3. Since rank S=2, it is possible to find a k-solution for $w' = 1$ and u' or $v' = 0$, if the linear form w' is not 0. If $w' = 0$ as a linear form, then we can find a solution for $u' = -v' = 1$. This means that $a_1 y_1^2 + a_2 y_2^2$ represents 1 over k, so $a_1 {y_1}^2 + a_2 {y_2}^2 - y^2$ represents 0. Conversely, suppose that $a_1 {y_1}^2 + a_2 {y_2}^2 - y^2$ represents 0 over k. If there is a solution with $y = 0$, then there is another with $y = 1$ (see [8], Appendix, Theorem 8). Let $n_1, n_2 \in k$ such that $a_1 {n_1}^2 + a_2 {n_2}^2 = 1$. We have then:

$$S = a_1 y_1^2 + a_2 y_2^2 = (a_1 n_1 y_1 + a_2 n_2 y_2)^2 + a_1 a_2 (n_1 y_2 - n_2 y_1)^2,$$

so S can be written as ${w'}^2 - u'v'$ with *rational* u', v', w'. This concludes the proof.

□

Remark 3.6. One sees that S will be of rank 2 iff $\mathcal{U} \sim \overline{\mathcal{U}}$ (recall that $\mathcal{U}$ is in general position).

Indeed, $\mathcal{U} \sim \overline{\mathcal{U}}$ iff it is equivalent to a sum of three Weierstrass points, which in turn corresponds to $W = 0$ and $F = -UV$. Now, S is of rank 2 iff it is equivalent over $\bar{k}$ to a form $-uv$.

Local-global principle Let k be a number field. Let X be a proper, geometrically integral variety defined over k. Then

$$\text{BP}\,(X, k) \Leftrightarrow \text{BP}\,(X_{k_v}, k_v) \text{ for every completion } k_v \text{ of } k.$$

Proof. See [4], Proposition 2.4. □

With no machinery but the Hasse principle for quadratic forms we can prove a particular case of the local-global principle.

Corollary 3.7. *Let k be a number field. The local-global principle holds for curves of genus* 2.

Proof. Let $[\mathcal{U}] \in \left(\mathrm{Pic}^3 \overline{\mathcal{C}}\right)^G$ such that $\mathcal{U}$ is a divisor in general position. Since $G_\nu = \mathrm{Gal}\,(\bar{k}_\nu / k_\nu) \subset G$, we have

$$[\mathcal{U}] \in \left(\mathrm{Pic}^3 \overline{\mathcal{C}}_\nu\right)^{G_\nu}.$$

Suppose that the quadratic form corresponding to $[\mathcal{U}]$ is of rank 3. By hypothesis, BP holds locally, and so by Proposition 3.5 the form $a_1 y_1^2 + a_2 y_2^2 + a_3 y_3^2$ represents 0 over k_ν and $-a_1 a_2 a_3$ is a square in k_ν for any place ν of k. By the Hasse principle the same is valid over k and again by Proposition 3.5 there is a rational divisor belonging to $[\mathcal{U}]$. Then BP holds ([4], remark after Lemma 3.4). Same proof for rank 2.

4. Finding rational classes and rational divisors

Let $\mathfrak{a} = (\theta, 0)$ be a Weierstrass point of $\mathcal{C}$. One has a commutative diagram

$$\begin{array}{ccc} \mathcal{J} & \xrightarrow{\psi_\theta} & \mathrm{Pic}^1 \overline{\mathcal{C}} \\ \Big\downarrow{\scriptstyle \xi} & & \Big\downarrow{\scriptstyle \eta} \\ \mathcal{K} & \xrightarrow[L_\theta]{} & \mathcal{K}^* \end{array}$$

where, for a divisor $\mathcal{U}$ of degree 0, we define $\psi_\theta([\mathcal{U}]) = [\mathcal{U} + \mathfrak{a}]$. Also, L_θ is a projective map from $\mathcal{K}$ to $\mathcal{K}^*$ defined over $k[\theta]$ (see [2], Lemma 4.5.1), and the columns are the quotient by $\pm Y$ involution. The diagram commutes because

$$\left[\overline{\mathcal{U} + \mathfrak{a}}\right] = \left[\overline{\mathcal{U}} + \overline{\mathfrak{a}}\right] = \left[\overline{\mathcal{U}} + \mathfrak{a}\right],$$

since $\overline{\mathfrak{a}} = \mathfrak{a}$.

Suppose $(\mathrm{Pic}^1 \overline{\mathcal{C}})^G \neq \emptyset$ and let $g_1, \ldots, g_s$ be generators of the Mordell-Weil group $\mathfrak{G}$, including those of the torsion part. We assert that there is a class $[\mathcal{V}] \in (\mathrm{Pic}^1 \overline{\mathcal{C}})^G$ such that, after renumbering $g_1, \ldots, g_s$, we have

$$[\mathcal{V} - \overline{\mathcal{V}}] = g_1 + \cdots + g_l \quad \text{in } \mathfrak{G}.$$

Indeed, let $[\mathcal{W}] \in (\mathrm{Pic}^1 \overline{\mathcal{C}})^G$, so $[\mathcal{W} - \overline{\mathcal{W}}] \in \mathfrak{G}$. Write then

$$[\mathcal{W} - \overline{\mathcal{W}}] = g_1 + \cdots g_l + 2 \sum c_i g_i.$$

Let $[\mathcal{U}] = \sum c_i g_i$. Then, since $[\mathcal{U} - \overline{\mathcal{U}}] = 2[\mathcal{U}]$ on the Jacobian, we have $[\mathcal{U} - \overline{\mathcal{U}}] = 2 \sum c_i g_i$. On taking $\mathcal{V} = \mathcal{W} - \mathcal{U}$, one gets

$$[\mathcal{V} - \overline{\mathcal{V}}] = g_1 + \cdots + g_l.$$

Lemma 4.1. *Let* $[\mathcal{V}] \in (\mathrm{Pic}^1 \overline{\mathcal{C}})^G$ *and denote by* h' *the logarithmic height on* $\mathbb{P}^3$. *Then*

$$h'(\eta([\mathcal{V}])) = \frac{1}{4} h'(\xi([\mathcal{V} - \overline{\mathcal{V}}])) + \mathcal{O}(1).$$

Proof. Since $[\mathcal{V} - \overline{\mathcal{V}}] = 2[\mathcal{V} - \mathfrak{a}]$ in the sense of the group law we have:

$$h([\mathcal{V} - \overline{\mathcal{V}}]) = 4h([\mathcal{V} - \mathfrak{a}]) + \mathcal{O}(1),$$

where h is the logarithmic height on $\mathcal{J} \subset \mathbb{P}^{15}$. Since ξ and L_θ are morphisms, of degree 2 and 1 respectively, one has

$$\begin{aligned} h'(\eta([\mathcal{V}])) &= h'(L_\theta \circ \xi([\mathcal{V} - \mathfrak{a}])) = h'(\xi([\mathcal{V} - \mathfrak{a}])) + \mathcal{O}(1) \\ &= 2h([\mathcal{V} - \mathfrak{a}]) + \mathcal{O}(1) = \frac{2}{4} h([\mathcal{V} - \overline{\mathcal{V}}]) + \mathcal{O}(1) \\ &= \frac{1}{4} h'(\xi([\mathcal{V} - \overline{\mathcal{V}}])) + \mathcal{O}(1)\,. \end{aligned}$$

□

This suggests that, if $(\mathrm{Pic}^1 \overline{\mathcal{C}})^G \neq \emptyset$ and if one can find decent generators for $\mathfrak{G}$, there will be a point $[\mathcal{V} - \overline{\mathcal{V}}] \in \mathfrak{G}$ whose height is not too big, and therefore a point $\eta([\mathcal{V}]) \in \mathcal{K}^*(k)$, of much smaller height, corresponding to a rational class. Conversely, points on $\mathcal{K}^*$ are easier to find and they may help finding generators for the Mordell-Weil group.

In practice this method turns out to be very efficient. Combined with Proposition 3.5 it allowed us to find very quickly rational divisors for all examples in the tables of Flynn [5]. Examples are available at the electronic adress below. Of course, we are not able to conclude in any case, that on a given curve there are *no* rational classes of degree 1. As long as one works only with curves having points everywhere locally, by the local-global principle we know that every rational class will have a rational divisor, but this is by no means needed to apply the method.

To illustrate this last remark, we take curves which do not have points everywhere locally. For instance, for any $p \neq 2$, choose integers $a,\ c$ which are non-squares mod p. Then the curve

$$Y^2 = c(X^2 - a)\left(X^2(X^2 - a) + p\right)$$

has no p-adic points, because the factors $X^2 - a$ and $X^2(X^2 - a) + p$ are at the same time squares or non-squares modulo p. We have run our programs for $a,\ c \leq p - 1$ (which is an arbitrary bound) and have looked for rational points on the surface K^* corresponding to each curve, actually in a fairly small range. We find primes, curves and points on the duals which correspond to rational classes with no rational divisor, and thus to curves for which BigPic fails. The Maple programs implementing the method as well as the results of the different computations made are available at

http://www.mat.ufmg.br/∼gonzalo/publications/rational/maple.htm

We now illustrate two applications of Proposition 3.5, one in rank 2 and one in rank 3 for the quadratic form S.

Example 4.2. Rank 2

The curve $\mathcal{C} : y^2 = 2(x^2+1)(x^2+4)(x^2+9)$ is a counter-example to the Hasse principle. It doesn't have rational points because its Jacobian is isogenous to the product of two elliptic curves of rank 0 and the torsion points of the elliptic curves do not come from rational points of $\mathcal{C}$. Denote $P_1 = (i, 0)$, $P_2 = (2i, 0)$ and $P_3 = (3i, 0)$. We have

$$\mathcal{U} = P_1 + P_2 + P_3 \sim (P_1 + P_2 + P_3)^\sigma$$

for every $\sigma \in G$, so $(\mathrm{Pic}^3 \overline{\mathcal{C}})^G$ and therefore $(\mathrm{Pic}^1 \overline{\mathcal{C}})^G$ is non-empty. By results of Siksek [7] or Skorobogatov [9] the Brauer-Manin obstruction is the only one.

The divisor $\mathcal{U}$ is given by

$$\begin{aligned} U(X) &= (X-i)(X-2i)(X-3i) \qquad \text{and} \quad Y = W(X) = 0 \\ &= X^3 - 6iX^2 - 11X + 6i = 0\,. \end{aligned}$$

The quadratic form obtained is

$$S = 72x_0^2 - 144x_0x_2 + 242x_1^2 - 44x_1x_3 + 72x_2^2 + 2x_3^2\,.$$

The rational divisor equivalent to $\mathcal{U}$ is given by

$$U'(X) = X^3 + 6X^2 - 11X - 6 = 0 \quad \text{and} \quad Y = W'(X) = 2X^3 - 22X\,.$$

The proper automorphism from $(U,\ V,\ W)$ to $(U',\ V',\ W')$ is given by:

$$\begin{pmatrix} U' \\ V' \\ W' \end{pmatrix} = \begin{pmatrix} \dfrac{1+i}{2} & \dfrac{-1+i}{4} & -i \\ 1-i & -\dfrac{1+i}{2} & -2i \\ 1 & -\dfrac{1}{2} & -i \end{pmatrix} \begin{pmatrix} U \\ V \\ 0 \end{pmatrix}.$$

This reflects the fact that the equivalence of the corresponding divisors is not given by a function defined over $\mathbb{Q}$. □

Example 4.3. Rank 3

To illustrate the rank 3 case, we take an example already considered by Flynn ([5], Example 3, page 446). Consider the curve

$$Y^2 = F(X) = -2X^6 - 2X^5 + 2X^4 + X^3 - 2X^2 - X + 2,$$

listed as $\mathcal{C}_{2U}$ in Flynn's tables. A quick search finds two rational points on the dual Kummer surface, namely $[-2 : -1 : 2 : 1]$ and $[-2 : 0 : 1 : 1]$, corresponding to the rational divisor classes listed in our tables. However, Flynn finds a rational class of degree 1 given by

$$R = \left[P_0 + (0\,,\ \sqrt{2}) - (-1\,,\ -\sqrt{2}) \right], \qquad \text{where}$$
$$P_0 = \left(\frac{7}{17} + \frac{4}{17}\sqrt{2}\,,\ -\frac{1888}{4913} + \frac{3465}{4913}\sqrt{2} \right).$$

By adding to R a canonical divisor expressed as $(-1\,,\ \sqrt{2}) + (-1\,,\ -\sqrt{2})$, we obtain a divisor of degree 3, in general position

$$\mathcal{U} = P_0 + (0\,,\ \sqrt{2}) + (-1\,,\ \sqrt{2})$$

whose class is rational. This divisor is given by $U(X) = 0$, $Y = W(X)$, where

$$U(X) = X(X+1)\left(X - \frac{7}{17} - \frac{4}{17}\sqrt{2} \right),$$
$$W(X) = \left(-\frac{2}{17} - \frac{6}{17}\sqrt{2} \right) X^2 + \left(-\frac{2}{17} - \frac{6}{17}\sqrt{2} \right) X + \sqrt{2}\,.$$

Here, $W(X)$ was found by imposing the curve $Y = W(X)$ to pass through $\mathcal{U}$. The algorithm and a simplification yield

$$F(X) = 1^2 - (X^3 - X + 1)(2X^3 + 2X^2 - 1) = W'^2 - U'V'.$$

The proper automorphism which sends $W^2 - UV$ to $W'^2 - U'V'$ is given by the matrix

$$C = \frac{1}{17}\left(A + B\sqrt{2} \right),$$

where

$$A = \begin{pmatrix} 7 & 5 & 2 \\ 20 & 7 & -4 \\ -2 & 1 & 3 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 4 & -2 & 6 \\ -8 & 4 & -12 \\ -6 & 3 & 8 \end{pmatrix}.$$

Comparing with the tables, we see that the initial class $[R]$ corresponds to the point $[-2 : -1 : 2 : 1]$ on the dual Kummer surface.

Acknowledgements. We thank the referee for his careful reading and several remarks which improved our paper.

References

[1] Bruin, N., Flynn, E.V.: Rational divisors in rational divisor classes. Algorithmic number theory. In proceedings of lecture notes in computer science 3079. Springer, Berlin Heidelberg New York, pp.132–139 (2004)

[2] Cassels, J.W.S., Flynn, E.V.: Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2. London Math. Soc. Lecture Note Series 230, Cambridge (1996)

[3] Cassels, J.W.S.: The Mordell-Weil group and curves of genus 2. Arithmetic and geometry. Papers dedicated to I.R. Shafarevich, 29–60, Vol I, Arithmetic. Birkhäuser, Boston,(1983)

[4] Coray, D., Manoil, C.: On large Picard groups and the Hasse Principle for curves and K3 surfaces. Acta Arith. **76**, 165–189 (1996)
[5] Flynn, E.V.: The Hasse principle and the Brauer-Manin obstruction for curves. Manuscripta Math. **115**, 437–466 (2004)
[6] Poonen, B., Schaefer, F.: Explicit descent for Jacobians of cyclic covers of the projective line. J. Reine Angew. Math. **488**, 141–188 (1997)
[7] Siksek, S.: On the Brauer-Manin obstruction for curves having split Jacobians. J. Theorie des Nombres de Bordeaux **16**, 773–777 (2004)
[8] Shafarevitch, I.R., Borevitch Z.I.: Théorie des nombres, Gauthier-Villars, Paris (1967)
[9] Skorobogatov, A.N.: Torsors and rational points. CTM, Cambridge University Press, Cambridge (2001)