A GEOMETRIC INTERPRETATION OF REDUCTION IN THE JACOBIANS OF C_{ab} CURVES.

RÉGIS BLACHE, JORGE ESTRADA SARLABOUS, AND MARIA PETKOVA

Abstract. In this paper, we show that the reduction of divisors in the Jacobian of a curve C can be performed by considering the intersections of a suitable projective model of C with quadrics in projective space. We apply this idea to certain projective model of elliptic and hyperelliptic curves on one hand, and to the canonical model of C_{ab} curves on the other hand, and we generalize (and recover) some well known algorithms.

AMS Subject Classification: 14H45, 14H40, 14Q05, 11G10, 11G20, 11T71

Key Words: C_{ab} Curves, Jacobian Varieties, Addition Law, Reduction Algorithm, Projective Model.

0. Introduction

The Jacobian varieties J of smooth projective curves of genus g, over the field k, with their natural group structure have always been an object of interest. First studied from theoretical point of view, they are in present of a practical interest in the construction of cryptosystems, based on the complexity of the discrete logarithm problem in the group of their rational points in the case of small genus.

The most famous example is the case of genus 1, when C is an elliptic curve isomorphic to J, and the group law is given by the well known "chord and tangent law". When C has genus greater than one, it is much more difficult to describe the Jacobian variety; it is possible to use a very ample line bundle coming from the theta divisor on J, but this gives an embedding in a projective space with dimension exponential in the genus of C, a fact which probably forbids efficient calculations over a projective model of J. To overcome this problem, we have to use another representation for the points of the Jacobian variety.

Many algorithms share an arithmetic approach of the addition of divisors, using the representations of C_{ab} curves by smooth affine equations and the fact that they have an unique point at infinity. Consequently the group $J(k)$ is canonically isomorphic to the ideal class group of the ring of regular functions over the affine model, and this is a Dedekind ring. Representing the ideals as finite dimensional modules over the ring $k[x]$ allows the use of the tools from algorithmic number theory. This approach has been applied to hyperelliptic curves in [3], superelliptic curves in [5], and C_{ab} curves in [7].

On the other hand, there are algorithms relying on a more geometrical point of view; addition of divisors modulo linear equivalence is a particular case of a more general process, namely reduction of divisors. If the curve C has a k-rational point P_∞, then any class of degree zero divisors modulo linear equivalence (i.e. any point in $J(\overline{k})$) has a unique representative of the form $D - dP_\infty$, with D a divisor of minimal degree $d \leq g$, the so called reduction. For instance, addition in the group of rational points of an elliptic curve is just reduction of divisors of the form $P + Q - 2P_\infty$. A natural idea is then to try to generalize the chord and tangent law. It is shown in [4] that when C is a trigonal curve of genus three, one can use intersections of the canonical model of C (in $\mathbb{P}^2$) with quadrics to reduce a divisor $E - 4P_\infty$ to a divisor $D - dP_\infty$, $d \leq 3$, and the same ideas are used for reduction over trigonal curves of genus four in [2].

The aim of this paper is to show that this point of view can be used to perform reduction in the Jacobian variety of any curve C (possessing a rational point). Considering the projective embeddings $\phi_\Delta(C)$ of C associated to very ample divisors of the form $\Delta = \delta P_\infty$, we isolate the properties of such an embedding that allow us to reduce a given divisor considering the intersections of $\phi_\Delta(C)$ with low degree hypersurfaces in the ambient projective space. We show that this is always possible when the embedding is projectively normal, in particular when Δ is a canonical divisor, or $\delta \geq 2g + 1$. Returning to the example of elliptic curves, we see that its Weierstrass model is exactly its embedding associated to the divisor $(2g + 1)P_\infty$, where P_∞ is the 0 of the group law. A consequence of our results is that considering the embedding $\phi_\Delta(C)$ of a curve C in $\mathbb{P}^{g+1}$ via the divisor $\Delta = (2g + 1)P_\infty$, and looking at the intersections of $\phi_\Delta(C)$ with hyperplanes allows the reduction of degree zero divisors of the form $D - (g + 1)P_\infty$; this seems a natural generalization of the chord and tangent law.

We also pay attention to the canonical model of a (non hyperelliptic) curve; it is also projectively normal, and allows us to use the geometrical interpretation of Riemann Roch theorem, in order to determine whether a given divisor is reduced or not, looking at its image via the canonical embedding. In the case of C_{ab} curves, we show that the divisor $(2g - 2)P_\infty$ (where P_∞ is the unique point obtained after desingularization of the point at infinity on the plane model of the curve) is a canonical divisor. This observation, joint with the ideas explained above, shows that this point of view is well suited for C_{ab} curves, and replaces the algorithms in [2], [4] in a more general context.

Another geometric approach of the addition in the Jacobian of a curve, based on the theory of Grassmanian varieties can be found in ([8], [9]).

The paper is organized as follows: in section 1, we recall well known facts that we use in the sequel; this includes properties of divisors and the Jacobian variety of a curve, and also of its projective embeddings. Then we define reduced divisors, give criterions for a divisor to be reduced and show that the reduction can be performed considering the intersections of a suitable projective embedding of the curve with hypersurfaces (*cf.* Lemma 1.4, Proposition 1.4). In section 2, we apply our results to elliptic and hyperelliptic curves, and show that they reduced to well known algorithms: the chord and tangent law and respectively the reduction part of Cantor's algorithm. In Proposition 2.1 we explain the reduction of a degree zero divisor of the form $D - (g + 1)P_\infty$ by intersections with hyperplanes in $\mathbb{P}^{g+1}$. In the last section, we apply our results to the canonical models of C_{ab} curves; we give a simple representative for the canonical divisor of such a curve, then we study the canonical model, give a criterion from linear algebra to decide whether a divisor is reduced or not, and discuss the reduction process on the Jacobian varieties of these curves.

1. Reduction of divisors and intersections of curves with low degree hypersurfaces.

We begin by setting some notations, and recalling some well known results. Let C be a complete nonsingular curve of genus g, defined over the field k. In the following, we assume that C has a k-rational point P_∞, that is $C(k) \neq \emptyset$. We denote by K_C the field of functions of C.

1.1. **Basic facts about divisors.** Recall that a *divisor* $D \in \mathrm{Div}(C)$ on C is a formal sum of points $D = \sum n_P P$, where the sum is taken over $C(\bar{k})$, and the n_P are almost all (that is all but a finite number) equal to zero; we denote by $\deg(D) = \sum n_P$ its *degree*, and by Supp $(D) := \{P \in C(\bar{k}),\ n_P \neq 0\}$ its *support*. There is a partial ordering in $\mathrm{Div}(C)$: for any two divisors $D = \sum n_P P$ and $D' = \sum n'_P P$ in $\mathrm{Div}(C)$, we have $D \geq D'$ when $n_P \geq n'_P$ for all $P \in C(\bar{k})$. We say that a divisor D is *effective* if $D \geq 0$, where 0 is the zero divisor, and that it is *affine* if its support doesn't contain P_∞.

If f is a function on C, recall that its divisor $(f) = (f)_0 - (f)_\infty$ is the sum of its zeroes and poles, counted with multiplicity; the divisor (f) has degree 0. The *principal divisors* are the divisors of functions in $K_C \otimes \bar{k}$. They form a group $\mathrm{Pr}(C)$ isomorphic to $\mathbb{P}(K_C \otimes \bar{k})$. The set of divisors $\mathrm{Div}(C)$ is an abelian group. In $\mathrm{Div}(C)$, the subset of degree 0 divisors forms a subgroup $\mathrm{Div}^0(C)$, and the set of principal divisors $\mathrm{Pr}(C)$ is a subgroup of $\mathrm{Div}^0(C)$. We say that two divisors D and D' are *linearly equivalent* if their difference is in $\mathrm{Pr}(C)$; we denote this by $D \sim D'$. The group $\mathrm{Pic}^0(C)$ is the group $\mathrm{Div}^0(C)/\mathrm{Pr}(C)$ of degree 0 divisors modulo linear equivalence; in the following we denote by $[D]$ the class in $\mathrm{Pic}^0(C)$ of the divisor $D \in \mathrm{Div}^0(C)$.

Let $G := \mathrm{Gal}(\bar{k}/k)$ be the absolute Galois group of k; since C is defined over k, G acts on the points of $C(\bar{k})$. In the following, the groups $\mathrm{Div}(C)(k) := \mathrm{Div}(C)^G$, $\mathrm{Pr}(C)(k) := \mathrm{Pr}(C)^G$, $\mathrm{Div}^0(C)(k) := \mathrm{Div}^0(C)^G$ and $\mathrm{Pic}^0(C)(k) := \mathrm{Pic}^0(C)^G$ denote the k-rational elements of the corresponding groups. Note that $\mathrm{Div}(C)(k)$ is *not* equal to the group generated by $C(k)$: points defined over an extension of k can appear, if all their conjugates over k appear with the same multiplicity. On the other hand, we have $\mathrm{Pr}(C)(k) = \mathbb{P}(K_C)$, as can be seen taking Galois cohomology of the exact sequence:

$$0 \to \bar{k}^* \to (K_C \otimes \bar{k})^* \to \mathrm{Pr}(C) \to 0,$$

with respect to G, and remarking that by Hilbert theorem 90, we have $H^1(G, \bar{k}^*) = \{1\}$.

Moreover, we have that $\mathrm{Pic}^0(C)(k) \simeq \mathrm{Div}^0(C)(k)/\mathrm{Pr}(C)(k)$; once more, take Galois cohomology of the exact sequence above; we see that by Hilbert theorem 90, and since G is also the Galois group of the extension $K_C \otimes \bar{k}/K_C$, we have $H^1(G, (K_C \otimes \bar{k})^*) = 0$; on the other hand, the group $H^2(G, \bar{k}^*)$ is canonically isomorphic to the Brauer group of the finite field k, which is trivial. Thus the group $H^1(G, \mathrm{Pr}(C))$ also vanishes. Finally, taking Galois cohomology of the sequence:

$$0 \to \mathrm{Pr}(C) \to \mathrm{Div}^0(C) \to \mathrm{Pic}^0(C) \to 0$$

shows that $\mathrm{Pic}^0(C)(k) \simeq \mathrm{Div}^0(C)(k)/\mathrm{Pr}(C)(k)$.

1.2. **Divisors on a curve and associated projective embeddings.** To every divisor D we can associate an invertible sheaf $\mathcal{L}(D)$ on C; we shall denote by $l(D)$ the dimension of the space of global sections

$$\Gamma(C, \mathcal{L}(D)) = \{f \in K_C,\ D + (f) \geq 0\},$$

and we have Riemann-Roch theorem: if K is a canonical divisor on C (i.e. the divisor of a differential form on C, of degree $2g - 2$), we have

$$\chi(\mathcal{L}(D)) := l(D) - l(K - D) = deg(D) + 1 - g.$$

The space $\mathbb{P}(\Gamma(C, \mathcal{L}(D)))$ is in one to one correspondance with the (complete) linear series $|D|$ of effective divisors linearly equivalent to D via the map $f \mapsto (f)+D$. The linear series $|D|$ associated to a divisor D define a morphism $\phi_D : C \mapsto \mathbb{P}^{l(D)-1}$; the divisor D is *very ample* when this morphism is a closed immersion; in this case the invertible sheaf $\mathcal{L}(D)$ is isomorphic to $\mathcal{O}_{\phi_D(C)}(1)$, and the linear series $|D|$ is the set of intersection divisors of $\phi_D(C)$ with the hyperplanes in $\mathbb{P}^{l(D)-1}$. Recall (cf [6] IV.5.2) that a *canonical divisor* K is very ample when C is a non hyperelliptic curve of genus $g \geq 2$, and defines the *canonical embedding* $\phi_K(C) \subset \mathbb{P}^{g-1}$. On the other hand, any divisor of degree $\geq 2g+1$ is very ample (cf [6] IV.3.3.2), and defines an embedding $\phi_D(C) \subset \mathbb{P}^{\deg(D)-g}$.

A closed subvariety $X \subset \mathbb{P}^n$ is *projectively normal* for the given embedding if its homogeneous coordinate ring is an integrally closed domain; in this case, the natural map $\Gamma(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(i)) \to \Gamma(X, \mathcal{O}_X(i))$ induced by taking global sections of the following exact sequence of sheaves:

$$0 \to \mathcal{I}_X(i) \to \mathcal{O}_{\mathbb{P}^n}(i) \to \mathcal{O}_X(i) \to 0$$

is surjective for all $i \geq 0$; thus we get the following exact sequence of k-vector spaces:

$$0 \to \Gamma(\mathbb{P}^n, \mathcal{I}_X(i)) \to \Gamma(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(i)) \to \Gamma(X, \mathcal{O}_X(i)) \to 0. \tag{1}$$

In the case X is the image $\phi_D(C)$ of a curve C as above, we can interpret this exact sequence in the following way: the first piece is the k-vector space of homogeneous polynomials of degree i in $k[X_0, \ldots, X_n]$ defining hypersurfaces containing $\phi_D(C)$; the second is the k-vector space of *all* homogeneous polynomials of degree i in $k[X_0, \ldots, X_n]$, and the last one is the k-vector space of global sections of the invertible sheaf $\mathcal{L}(iD)$, it corresponds as above to the linear series $|iD|$ of intersection divisors of $\phi_D(C)$ with hypersurfaces of degree i in $\mathbb{P}^n$.

Now it is a classical result of Enriques and Petri that the image of the canonical embedding of a curve is projectively normal; on the other hand, if D is a divisor of degree greater than or equal to $2g+1$, then $\phi_D(C)$ is also projectively normal (cf [11] p. 55).

We end this paragraph by recalling a geometric interpretation of Riemann-Roch theorem. For an effective divisor D, the geometric interpretation of $l(K-D)$ is the following: consider the canonical embedding of C in $\mathbb{P}^{g-1}$; then $l(K-D)$ is the dimension of the k-vector space of linear polynomials in $k[X_0, \ldots, X_{g-1}]$ defining hyperplanes in $\mathbb{P}^{g-1}$ whose intersection divisor with $\phi_K(C)$ is greater or equal than D.

1.3. **Reduced divisors on a curve.** Recall (cf [10]) that the *Jacobian of* C, J_C is the abelian variety representing the functor $P_C^0 : T \mapsto P_C^0(T)$ from schemes over k to abelian groups, where $P_C^0(T)$ is the group of families of invertible sheaves on C of degree 0 parametrized by T, modulo the trivial families. In particular, from our assumption that C has a k-rational point P_∞, the k rational points of J are the elements of $\mathrm{Pic}_C^0(k)$, i.e. the group of k-rational degree 0 divisors up to linear equivalence (cf. [10] p. 168). It is in this group that we wish to make calculations; we first need a lemma to give a more handy description of its elements.

Lemma 1.1. *Let $E \in \mathrm{Div}^0(C)(k)$ be a k-rational degree 0 divisor on C. There is an affine effective k-rational divisor E' of degree $\leq g$ on C such that $E \sim E' - \deg(E')P_\infty$.*

Proof: This is an application of Riemann-Roch theorem: consider the degree g divisor $F := E + gP_\infty$; we clearly have $l(F) \geq 1$. If $f \in l(F)\backslash\{0\}$, then the divisor $F' := (f) + F = (f) + E + gP_\infty$ is effective of degree g. Let m_∞ be its multiplicity at P_∞; then $m_\infty \leq g$, and the divisor $E' := F' - m_\infty P_\infty$ satisfies the requirements of the lemma. □

Thus every point in $J_C(k)$ can be represented by an affine effective divisor of degree $\leq g$. Note that this is a well-known fact, since the Jacobian of C is the unique abelian variety birationnally equivalent to the g-th symmetric power of C, $C^{(g)}$ (cf. [10] Remark 5.6). Unfortunately, if $g \geq 2$, this birational equivalence is not an isomorphism, and the above representation is not unique. Nevertheless, this representation is unique if we ask E' to be of minimal degree; the following lemma is Theorem 1 of [5]

Lemma 1.2. *Let $E \in \mathrm{Div}^0(C)(k)$ be a k-rational degree 0 divisor on C. There is a unique effective divisor E' over k of minimal degree $d \leq g$ such that $E \sim E' - dP_\infty$.*

We can now define the reduction of a divisor:

Definition 1.1. *Let E be a degree 0 divisor on C; the* reduction *of E is the unique divisor, linearly equivalent to E, of the form $E' - \deg(E')P_\infty$, with E' affine effective of minimal degree. A divisor is called* reduced *if it is its own reduction.*

We now give a condition for a divisor $E - \deg(E)P_\infty$, E affine effective and $\deg(E) \leq g$ to be reduced

Lemma 1.3. *Let $E - eP_\infty$, a degree 0 divisor, with E affine effective of degree $e \leq g$. It is not reduced if and only $l(E) \geq 2$.*

Proof: Assume first that $E - eP_\infty$ is not reduced: we can find a degree 0 divisor $E' - e'P_\infty$, E' affine effective, $e' < e$, such that $E' - e'P_\infty \sim E - eP_\infty$, and a function f on C such that $(f) = E' + (e - e')P_\infty - E$. Thus f is a non constant function in $\Gamma(C, \mathcal{L}(E))$, and since E is effective, we get $l(E) \geq 2$. Conversely, if $l(E) \geq 2$, we get a non constant function f in $\Gamma(C, \mathcal{L}(E))$, thus having no pole at P_∞. Set $f_0 := f - f(P_\infty)$, and $E' := (f_0) + E$; since f_0 is not constant, $E \neq E'$. Moreover the divisor (f_0) has positive multiplicity at P_∞; we get $E - eP_\infty \sim E' - e'P_\infty$ with $e' < e$, and $E - eP_\infty$ is not reduced. □

We give a geometric condition for a divisor $E - \deg(E)P_\infty$, E affine effective and $\deg(E) \leq g$ to be reduced. In the case of hyperelliptic curves, it is well know that such a divisor is reduced unless the support of E contains two points conjugate under the hyperelliptic involution. For nonhyperelliptic curves, the canonical embedding and the geometric interpretation of Riemann-Roch theorem allow us to characterise these divisors

Proposition 1.1. *Let C be a nonhyperelliptic curve, and $E - eP_\infty$, a degree 0 divisor, with E affine effective of degree $e \leq g$. It is not reduced if and only the (projective) dimension of the intersection of hyperplanes H in $\mathbb{P}^{g-1}$ such that $H \cdot \phi_K(C) \geq E$ is less than $e - 1$.*

Proof: Assume $E - eP_\infty$ is not reduced. From lemma 1.3, $l(E) \geq 2$. Thus Riemann Roch theorem ensures $l(K - E) > g - e$. Recall the geometric interpretation of the number $l(K - E)$: it is the dimension of the space of hyperplanes in $\mathbb{P}^{g-1}$ whose intersection divisor with $\phi_K(C)$ is greater or equal than E. Thus these hyperplanes form a subspace W_E of dimension greater than $g-e$ in the dual projective space $\mathbb{P}^{g-1*}$; since the intersection of these hyperplanes is the subspace of $\mathbb{P}^{g-1}$ dual to W_E, we get the result. Assume conversely that the dimension of the space in the proposition is less than $e-1$; then Riemann Roch theorem gives $l(E) \geq 2$, and this ends the proof of the proposition with the help of lemma 1.3. □

Finally, we describe the functions in $\Gamma(C, \mathcal{L}(E))$, E affine effective of degree $e \leq g$ such that $E - eP_\infty$ is not reduced, in terms of the hyperplanes in $\mathbb{P}^{l(D)-1}$, $D = dP_\infty$ with $d \geq 2g+1$ or $d = 2g-2$ if this is a canonical divisor. If L is a linear polynomial in $X_0, \dots, X_{l(D)-1}$, we denote by H_L the associated hyperplane in $\mathbb{P}^{l(D)-1}$.

Proposition 1.2. *Let $E - eP_\infty$, E affine effective of degree $e \leq g$ a non reduced divisor. Then there is an hyperplane H_0 in $\mathbb{P}^{l(D)-1}$ such that $H_0 \cdot \phi_D(C) = E + E' \geq E$. Let L_0 be a linear polynomial defining H_0; we have*

$$\Gamma(C, \mathcal{L}(E)) = \left\{ f = \frac{L}{L_0},\ H_L \cdot \phi_D(C) \geq E' \right\}.$$

Proof: First note that if $\deg D \geq 2g+1$, then $l(D) \geq g+2$, and there is an hyperplane H_0 as in the proposition. If D is a canonical divisor, this claim comes from proposition 1.1. In any case, since $E \leq H_0 \cdot \phi_D(C)$, we have $\Gamma(C, \mathcal{L}(E)) \subset \Gamma(C, \mathcal{L}(H_0 \cdot \phi_D(C)))$. Now the map

$$\Gamma(\mathbb{P}^{l(D)-1}, \mathcal{O}_{\mathbb{P}^{l(D)-1}}(1)) \to \Gamma(C, \mathcal{L}(H_0 \cdot \phi_D(C)))$$

is an isomorphism: it is surjective since $\phi_D(C)$ is projectively normal, and these vector spaces have dimension $l(D)$. It maps the linear polynomial L to the function $\frac{L}{L_0}$. Finally, this function is in $\mathcal{L}(E)$ if and only if $H_L \cdot \phi_D(C) - H_0 \cdot \phi_D(C) + E \geq 0$, i.e. if and only if $H_L \cdot \phi_D(C) \geq E'$. □

1.4. **Reduction and intersections with hypersurfaces.** Here we fix once and for all a divisor $D = dP_\infty$, $d \geq 2g+1$ or $d = 2g-2$ if D is a canonical divisor; note that in any case the divisor D is very ample and the image $\phi_D(C)$ is projectively normal. Our aim in this paragraph is to show that we can find the reduction of a divisor $E - \deg(E)P_\infty$ with E affine effective of degree $\deg(E) \leq kd - g$, by considering intersections of $\phi_D(C)$ with hypersurfaces of degree k in $\mathbb{P}^{l(D)-1}$.

Lemma 1.4. *Let E be an affine effective divisor of degree $e \leq kd - g$. Then there is a hypersurface Q_E of degree k in $\mathbb{P}^{l(D)-1}$ such that:*

$$Q_E \cdot \phi_D(C) \geq E + (kd - g - e)P_\infty,$$

where $Q_E \cdot \phi_D(C)$ is the intersection divisor of Q_E and C in $\mathbb{P}^{l(D)-1}$.

Proof: Since Q_E has degree k, the intersection divisor $Q_E \cdot C$ is linearly equivalent to kD, that is $Q_E \cdot \phi_D(C) = kD + (f)$; thus the condition of the lemma can be rewritten $kD + (f) \geq E + (kd - g - e)P_\infty$, and we are reduced to look for a function f in $\Gamma(C, \mathcal{L}((g+e)P_\infty - E))$, since $D = dP_\infty$.

Because of $kD \geq (g+e)P_\infty - E$, we certainly have the inclusion $\Gamma(C, \mathcal{L}((g+e)P_\infty - E) \subset \Gamma(C, \mathcal{L}(kD))$. From Riemann-Roch theorem, since $\deg((g+e)P_\infty - E) = g$, we have $l((g+e)P_\infty - E)) \geq 1$. Let f_E be a non zero function in $\Gamma(C, \mathcal{L}((g+e)P_\infty - E)) \subset \Gamma(C, \mathcal{L}(kD))$, and V_E a preimage of f_E by the third arrow of:

$$0 \to \Gamma(\mathbb{P}^n, \mathcal{I}_C(k)) \to \Gamma(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(k)) \to \Gamma(C, \mathcal{O}_C(k)) \to 0.$$

Clearly the hypersurface Q_E with homogeneous equation V_E satisfies the requirements of the lemma. □

We now show that the reduction of divisors can be performed by considering intersections of $\phi_D(C)$ with suitable hypersurfaces. We begin by divisors of the form $E - eP_\infty$, $e \leq g$. If this divisor is not reduced, then there is an hyperplane H_E such that $H_E \cdot \phi_D(C) \geq E$ (this follows from lemma 1.4 if $d \geq 2g+1$, and from proposition 1.1 if D is a canonical divisor). Then $H_E \cdot \phi_D(C) = E + E'$; let $H_{E'}$ be an hyperplane such that $H_{E'} \cdot \phi_D(C) \geq E'$, and $H_{E'}$ has maximal intersection multiplicity with $\phi_D(C)$ at $\phi_D(P_\infty)$ among the hyperplanes having that property.

In the general case, let Q_E be an hypersurface as in lemma 1.4. By Bezout's theorem, the divisor $Q_E \cdot \phi_D(C)$ has degree kd, and it can be written:

$$Q_E \cdot \phi_D(C) = E + E' + (kd - g - e)P_\infty,$$

with E' a divisor of degree g. Applying once more lemma 1.4, we see that there exists an homogeneous polynomial $V_{E'}$ of degree $l \leq 2$ ($l = 1$ except if D is a canonical divisor), defining a degree l hypersurface $Q_{E'}$, such that $Q_{E'} \cdot \phi_D(C) \geq E' + (ld - 2g)P_\infty$. We get $Q_{E'} \cdot \phi_D(C) = E' + E'' + (ld - g - e'')P_\infty$, with E'' an effective divisor of degree $e'' \leq g$ on C.

Proposition 1.3. *The divisor $E'' - e''P_\infty$ is linearly equivalent to $E - eP_\infty$.*

Proof. We first show that these two divisors are linearly equivalent. First consider the function $v_E := \frac{V_E}{X_0^k}$; its divisor is:

$$(v_E) = Q_E \cdot C - kH_0 \cdot C = E + E' - (g + e)P_\infty,$$

where H_0 is the hyperplane with equation $X_0 = 0$. Now the function $v_{E'} := \frac{V_{E'}}{X_0^2}$ has divisor:

$$(v_{E'}) = Q_{E'} \cdot C - 2H_0 \cdot C = E' + E'' - (g + e'')P_\infty.$$

Thus the function $v_E/v_{E'}$ has divisor $(v_E) - (v_{E'}) = E - E'' + (e'' - e)P_\infty$. □

The divisor $E'' - e''P_\infty$ is not necessarily reduced; let us show that we can reduce it by considering the intersection of $\phi_D(C)$ with hyperplanes in $\mathbb{P}^{l(D)-1}$. If it is reduced, there is nothing to do; else let H_0 be an hyperplane such that $H_0 \cdot \phi_D(C) = E'' + F' \geq E''$. Such an hyperplane exists from proposition 1.2. Let H_1 be the hyperplane such that $H_1 \cdot \phi_D(C) \geq F'$, and whose intersection multiplicity with $\phi_D(C)$ at $\phi_D(P_\infty)$ is maximal; if we set $H_1 \cdot \phi_D(C) = F' + F + sP_\infty$, with $\deg(F) = f$, we have

Proposition 1.4. *The divisor $F - fP_\infty$ is the reduction of $E'' - e''P_\infty$ (and of $E - eP_\infty$).*

Proof: As in the proof of proposition 1.3, we get that $F - fP_\infty$ is linearly equivalent to $E'' - e''P_\infty$ (their difference is $H_1 \cdot \phi_D(C) - H_0 \cdot \phi_D(C)$). On the other hand, if $E_0 - e_0P_\infty$ is the reduction of $E'' - e''P_\infty$, we get a function f_0 whose divisor is $E_0 + (e'' - e_0)P_\infty - E''$. From the definition of reduced divisors, this is the function in $\Gamma(C, \mathcal{L}(E''))$ with a zero of maximal order at P_∞. From the description of the functions of $\Gamma(C, \mathcal{L}(E''))$ in proposition 1.2, we get $(f) = H_1 \cdot \phi_D(C) - H_0 \cdot \phi_D(C)$. □

2. The case of elliptic and hyperelliptic curves.

The aim of this section is to illustrate the results above in the case of elliptic and hyperelliptic curves; note that in both cases, the canonical divisor is *not* very ample, since it has degree 0 in the first case, and is a multiple of the g_2^1 in the second (cf [6] IV.5.2). Thus in both cases (assuming once again that our curves have a rational point P_∞), we use the projective embedding induced by the divisor $(2g+1)P_\infty$, which is always very ample, and whose image is projectively normal. We will see that if we wish to reduce an effective divisor of degree $g+1$ to a linearly equivalent effective divisor of degree g, our method reduces to the chord and tangent law in the case of elliptic curves, and to the reduction part of Cantor's algorithm (cf [3] §4) in the hyperelliptic case.

2.1. Elliptic curves.

Recall that in the case of an elliptic curve (of genus 1) having a k-rational point P_∞, the set $J_C(k)$ can be identified to $C(k)$ via the one-to-one correspondance $P \mapsto [P - P_\infty]$; in fact the group law on $C(k)$ is induced by the one on $J_C(k)$: if we have $[R - P_\infty] = [P - P_\infty] + [Q - P_\infty]$ in $J_C(k)$ for three points P, Q, R in $C(k)$, then setting $R = P \oplus Q$ on $C(k)$ defines a group law, for which the identity is P_∞. The aim of this paragraph is to explain that proposition 1.4 just describes the well-known chord and tangent law.

Let C be a complete nonsingular curve of genus 1, with a rational point $P_\infty \in C(k)$. The divisor $D := 3P_\infty$ is very ample, and since it is non special, we have $l(D) = 2$ by Riemann-Roch theorem. Consequently the morphism $\phi_D : C \to \mathbb{P}^2$ is a closed immersion, and its image is a nonsingular cubic curve in $\mathbb{P}^2$. In this case Proposition 1.4 can be rewritten as follows.

Proposition 2.1. *Assume that $D = (2g+1)P_\infty$; then we can perform the reduction of a divisor $E - (g+1)P_\infty$, with E affine effective of degree $g+1$ considering the intersection of $\phi_D(C)$ with hyperplanes in $\mathbb{P}^{g+1}$.*

Let $E = P + Q$ be a divisor of degree 2; there is a hyperplane in $\mathbb{P}^2$ (i.e. a line) passing through P and Q (note that if $P = Q$ we have to take the tangent line to C at P); it meets $\phi_D(C)$ at a third point E'. Now the line in $\mathbb{P}^2$ passing through E' and P_∞ is the "vertical" line with equation $x = x_{E'}$; it meets C at a third point E'' with coordinates $(x_{E'}, y_{E'})$, and $E'' - P_\infty$ is the reduction of $E - 2P_\infty$.

To summarize what we have just said, we get: $[E'' - P_\infty] = [P + Q - 2P_\infty] = [P - P_\infty] + [Q - P_\infty]$, i.e. via the identification above $E'' = P \oplus Q$; on the other hand, the geometric process that we have described is just the natural way of adding points on an elliptic curve, the chord/tangent law.

2.2. Hyperelliptic curves.

An *hyperelliptic curve* is a curve C of genus $g \geq 2$ such that there exists a morphism $C \to \mathbb{P}^1$ of degree 2. In other words, it is a curve whose function field is a quadratic extension of the rational function field. Here we restrict our attention to the curves having a plane affine model C_{aff} with equation

$$y^2 + h(x)y = f(x)$$

where $h(x)$ is a polynomial of degree at most g, and $f(x)$ a monic polynomial of degree $2g+1$. Note that if the characteristic of k is not 2, we can take $h(x) = 0$. We assume moreover that the affine model above is nonsingular; if $h(x) = 0$, this reduces to ask f to have only simple roots in $\overline{k}$, the algebraic closure of k.

The projective closure of C_{aff} above in $\mathbb{P}^2$ has a unique (singular) point at infinity, which is rational over k; we shall denote it by P_∞. From the theory of algebraic function fields of one variable, we get that the function x (*resp.* y) has a pole of order 2 (*resp.* $2g+1$) at P_∞. Thus we get

$$\mathcal{L}((2g+1)P_\infty) = \mathrm{Vect}(1, x, \ldots, x^g, y).$$

Let us describe precisely $\phi_D(C)$, the embedding of C in $\mathbb{P}^{g+1}$ induced by the divisor D. Let $X_0, \ldots, X_{g+1}$ be a system of homogeneous coordinates in $\mathbb{P}^{g+1}$. A point with coordinates (x, y) of the affine plane model is sent to the point with homogeneous coordinates $(1 : x : \cdots : x^g : y)$ in $\mathbb{P}^{g+1}$. The point at infinity is sent to the point $\mathcal{P}_\infty$ with homogeneous coordinates $(0 : \cdots : 0 : 1)$; moreover ϕ_D is an isomorphism between C_{aff} and $\phi_D(C)\backslash\{\mathcal{P}_\infty\}$, and the hyperelliptic involution is the map on $\phi_D(C)$ sending $P(1 : x : \cdots : x^g : y)$ to $\sigma(P)(1 : x : \cdots : x^g : -y)$.

Let us compute the intersection multiplicity I_i, $0 \leq i \leq g$ of the hyperplane H_i with equation $X_i = 0$ with $\phi_D(C)$ at $\mathcal{P}_\infty$. Since this point is not on H_{g+1}, I_i is the multiplicity of $\mathcal{P}_\infty$ in the divisor of the function X_i/X_{g+1}; via ϕ_D, this function corresponds to $x^i y^{-1}$, whose order at P_∞ is $2(g-i)+1$. Finally we get $I_i = 2(g-i)+1$.

We are now ready to apply the reduction procedure of Proposition 1.4. Assume that we have two reduced divisors $D_1 - gP_\infty$ and $D_2 - gP_\infty$ with D_1, D_2 affine effective of respective degree g. We wish to reduce the divisor $D_1 + D_2 - 2gP_\infty$; from lemma 1.3, we can find a quadric Q in $\mathbb{P}^{g+1}$ such that $Q \cdot \phi_D(C) \geq D_1 + D_2 + (g+2)\mathcal{P}_\infty$. The condition $Q \cdot \phi_D(C) \geq (g+2)\mathcal{P}_\infty$ ensures that the only monomials appearing in the homogeneous equation of Q are the $X_i.X_j$, $I_i + I_j \geq g+2$. From the above computation of intersection numbers, we get that $2(i+j) \leq 3g$. Via ϕ_D, we see that we just have to consider polynomials in $k[x, y]$ of the form $c(x) + d(x)y$, with $\deg(c) \leq \frac{3g}{2}$ and $\deg(d) \leq \frac{g-1}{2}$. Once again, by Bezout's theorem, we get an effective divisor E' of degree g such that $Q.\phi_D(C) = E' + D_1 + D_2 + (g+2)\mathcal{P}_\infty$. Applying once more Lemma 1.3, we get an hypersurface H passing through $\mathcal{P}_\infty$ (i.e. in which homogeneous equation the variable X_{g+1} doesn't appear), and E'' an effective divisor of degree g such that $E'' - g\mathcal{P}_\infty$ is the reduction of $D_1 + D_2 - 2g\mathcal{P}_\infty$. Note that in this case the last step is trivial: assume that $E' = \sum n_i P_i$, with $P_i(1 : x_i : \cdots : x_i^g : y_i)$. Then we have $E'' = \sigma(E') = \sum n_i \sigma(P_i)$.

3. The case of C_{ab} curves, $a, b \neq 2$.

3.1. **Definition and first results.** In this part, we begin by defining a large class of curves, the C_{ab} curves; then we compute their genus and their canonical divisor.

Definition 3.1. *Let a, b be coprime integers; assume moreover that they are prime to the characteristic of the base field k, and that $a > b$. A C_{ab}* curve *is a curve having an irreducible affine nonsingular plane model with equation:*

$$P_{ab}(x, y) = \sum \alpha_{ij} x^i y^j = 0,$$

where the sum is taken over couples $(i, j) \in \{0, \ldots, b\} \times \{0, \ldots, a\}$ such that $ai + bj \leq ab$, and $\alpha_{b0}\alpha_{0a} \neq 0$.

Let C be a C_{ab}-curve, and $K_{ab} = k(x, y)$ be its function field; since a and b are coprime integers, the extension $K_{ab}/k(x)$ ramifies totally above the point at infinity; we get a unique pont, that we shall denote P_∞ in the sequel. It is well known that the genus of C is:

$$g = \frac{(a-1)(b-1)}{2}.$$

Recall the notion of Weierstrass integers (cf. [1]): if C is a curve of genus g, and $P \in C(k)$ a k-rational point of C, then we have a sequence of $2g$ k-vector spaces:

$$k = \Gamma(C, \mathcal{L}(0)) \subset \Gamma(C, \mathcal{L}(P)) \subset \cdots \subset \Gamma(C, \mathcal{L}((2g-1)P)),$$

the last one being of dimension g by Riemann-Roch theorem; considering the dimensions of these vector spaces, we have the following inequalities:

$$1 = l(0) \leq l(P) \leq l(2P) \leq \cdots \leq l((2g-1)P) = g$$

Again by Riemann-Roch theorem, we have $l(iP) - l((i-1)P) \leq 1$; thus for g non negative integers $0 = n_0, \dots, n_{g-1} \leq 2g-1$, we have $l(iP) = l((i-1)P) + 1$ (i.e. there is a function $f \in K_{ab}$ whose polar divisor $(f)_\infty$ is iP). The sequence:

$$n_0 := 0, n_1 := b, \dots, n_{g-1}, 2g, 2g+1, \dots$$

is called the *sequence of Weierstrass integers of* C *at* P; it is a semigroup in $\mathbb{N}$. The remaining g integers (for which we have $l(iP) = l((i-1)P)$) are called the *gaps of* C *at* P.

In the case of C_{ab} curves, we can easily describe the sequence of Weierstrass integers at P_∞

Lemma 3.1. *The semigroup of Weierstrass integers at* P_∞ *of a* C_{ab}*-curve is* $H_{ab} := a\mathbb{N} + b\mathbb{N}$.

Proof: Since $(x)_\infty = aP_\infty$, and $(y)_\infty = bP_\infty$, we clearly see that H_{ab} is contained in the sequence of Weierstrass integers; moreover the functions on C whose only pole is P_∞ are the function of $k[x,y] := \Gamma(C \backslash \{P_\infty\}, \mathcal{O}_C) = k[X,Y]/(P_{ab})$, and the above inclusion is in fact an equality. □

We can now use this result to give the last gap of C at P_∞, and to determine the canonical divisor of C.

Proposition 3.1. *i) The* $g-1$*-th Weierstrass integer of* C *at* P_∞ *is* $n_{g-1} = 2g-2$;
ii) The last gap of C *at* P_∞ *is* $2g-1$;
iii) Let K *be a canonical divisor of* C*; we have:* $K \sim (2g-2)P_\infty$.

Proof: *i)* From lemma 3.1, it is sufficient to show that $2g-2 \in a\mathbb{N} + b\mathbb{N}$. Since a and b are coprime positive integers, we can write $au - bv = 1$, for some $0 < u < b$, $0 < v < a$. Thus

$$2g-2 = ab - a - b - 1 = ab - (u+1)a + (v-1)b = (b-u-1)a + (v-1)b,$$

and we get the result.

ii) If we write $2g-1 = (b-1)a - b$, all the other expressions of this integer as a linear combination of a and b with integer coefficients are of the form $((1-n)b-1)a + (na-1)b$, $n \in \mathbb{Z}$; since $a, b \geq 3$, the integers $(1-n)b-1$ and $na-1$ cannot be simultaneously nonnegative, and the result follows from lemma 3.1 and the discussion above.

iii) We apply Riemann-Roch theorem to the divisors $(2g-2)P_\infty$ and $(2g-1)P_\infty$:

$$l((2g-2)P_\infty) - l(K - (2g-2)P_\infty) = g-1;$$
$$l((2g-1)P_\infty) - l(K - (2g-1)P_\infty) = g.$$

Since $2g-1$ is a gap for C at P_∞, we have $l((2g-2)P_\infty) = l((2g-1)P_\infty)$; on the other hand, $l(K-(2g-1)P_\infty) = 0$ as this divisor has degree -1. Thus we get $l(K - (2g-2)P_\infty) = 1$. But this last divisor has degree 0, hence it must be the divisor of a rational function, and we obtain in this way the desired linear equivalence. □

3.2. **Geometry of the plane and canonical models of a C_{ab} curve.** Let C be a C_{ab}-curve; we denote by $\phi(C)$ the projective closure (in $\mathbb{P}^2$) of the affine plane model given in the definition; note that $\phi(C)$ has a unique point at infinity (the point with homogeneous coordinates $(1:0:0)$ since we assumed $a>b$), and that it is in general singular, except if $|a-b|\leq 1$. Remark that ϕ is the morphism defined by the linear system corresponding to the sub-vector space $\mathrm{Vect}(1,x,y)\subset\Gamma(C,\mathcal{L}(aP_\infty))$.

Let $\phi_K(C)$ be the image of C by the projective embedding $\phi_K : C\to\mathbb{P}^{g-1}$ induced by the divisor $(2g-2)P_\infty \sim K$. To be more precise, we set $\Gamma(C,\mathcal{L}((2g-2)P_\infty)$ $=\mathrm{Vect}(f_0,\ldots,f_{g-1})$, where the f_i are monomials in x, y, ordered by increasing pole order at P_∞ (note that $v_{P_\infty}(f_i) = n_i$, the $(i+1)$-th Weierstrass integer). For each point P of the curve, its image is $\phi_K(P) = ((t^{e_P}f_0)(P):\cdots:(t^{e_P}f_{g-1})(P))$, where $e_P = -\min(v_P(f_0),\ldots,v_P(f_{g-1}))$, and t is a local parameter for C at P. Note that $e_P=0$ for all points of C except P_∞; then $e_P = 2g-2$. In particular the image of P_∞ by this embedding is the point $P_{K,\infty} := \phi_K(P_\infty)$ with homogeneous coordinates $(0:\cdots:0:1)$ in $\mathbb{P}^{g-1}$.

We now describe a system of generators for the canonical ideal, i.e. the homogeneous ideal $I_{C,K}$ of $\phi_K(C)$ in $k[X_0,\ldots,X_{g-1}]$: following the work of Petri (cf. [12]), we obtain that the canonical ideal is generated by the quadrics

$$X_iX_j = X_kX_l \text{ if } n_i+n_j = n_k+n_l.$$

and a homogeneous polynomial $\mathcal{P}_{ab}$ which is a quadric if C is not trigonal nor the smooth plane quintic, a cubic else. In case it is a quadric, we can write it

$$\mathcal{P}_{ab}(X_i) = \sum \alpha_{ij}X_rX_s, \quad \text{for some} \quad r,s, \quad \text{such that} \quad n_r+n_s = ai+bj.$$

Now we have the isomorphism of affine curves:

$$\begin{array}{cccc} \phi & : & \phi(C)\backslash\{P_\infty\} & \to & \phi_K(C)\backslash\{P_{K,\infty}\} \\ & & P=(x:y:1) & \mapsto & (1:x^iy^j, ai+bj\leq 2g-2), \end{array}$$

which is just the geometric version of the following isomorphism of k-algebras, where $I'_{C,K}$ is the ideal obtained from $\mathcal{I}_{C,K}$ by dehomogenization with respect to X_0:

$$\begin{array}{cccc} \phi^\# & : & k[x_1,\ldots,x_{g-1}]/I'_{C,K} & \to & k[x,y]/(P_{ab}) \\ & & x_l & \mapsto & x^iy^j,\ n_l = ai+bj. \end{array}$$

Note that this morphism is well defined since each of the Weierstrass integers $n_0,\ldots,n_{g-1}$ has a unique representation as an element of $a\mathbb{N}+b\mathbb{N}$.

We end this paragraph computing the intersection numbers at P_∞ of $\phi_K(C)$ with any hyperplane in $\mathbb{P}^{g-1}$

Lemma 3.2. *Let H be the hyperplane defined by the equation $a_0X_0+\cdots+a_{g-1}X_{g-1}=0$. We have:*

$$I_{P_\infty}(C_{ab},H) = 2g-2-n_l,\ l=\max\{i\in\{0,\ldots,g-1\},\ a_i\neq 0\}.$$

Proof: It is well known that

$$I_{P_{K,\infty}}(H,\phi_K(C)) = v_{P_\infty}(a_0f_0+\cdots+a_{g-1}f_{g-1}) + e_{P_\infty},$$

where $f_0,\ldots,f_{g-1}$ are the functions defining the projective morphism ϕ_K, and $e_{P_\infty} = 2g-2$ is as above; since $v_{P_\infty}(f_i) = n_i$, and these numbers are pairwise distinct, we get the result. □

3.3. **Reduced divisors on C_{ab}-curves.** In this paragraph, we give a criterion for deciding whether a divisor of degree $\leq g$ is reduced, using the geometric interpretation of Riemann-Roch theorem on the canonical model; to such a divisor we associate a matrix, which has maximal rank exactly when the divisor is reduced.

In order to do this, we recall the notion of an *osculating plane* for $\phi_K(C)$: the k-th osculating space for $\phi_K(C)$ at P, $V_k(P)$, is the projective subspace of $\mathbb{P}^{g-1}$ of minimal dimension such that $V_k(P)\cdot\phi_K(C)\geq kP$; this is also the intersection of the hyperplanes in $\mathbb{P}^{g-1}$ intersecting $\phi_K(C)$ at P with multiplicity at least k. Note that our definition is slightly different from the one in [13]; actually the two definition coincide when the first k Weierstrass gaps at P are $0,1,\cdots,k-1$.

We need a system of points in $\mathbb{P}^{g-1}$ spanning this space. Recall from [13] the definition of *Hasse derivatives*; the i-th Hasse derivative, $D^{(i)}$, is defined on $k[x]$ by $D^{(i)}(\sum a_jx^j):=\sum\binom{j}{i}a_jx^{j-i}$, and extends to $k(x)$ and its separable extensions. Then it is well know (*cf.* [13] Theorem 1.1) that the points with homogeneous coordinates $((D^{(i)}f_0)(P):\cdots:(D^{(i)}f_{g-1})(P))$, $0\leq i\leq k-1$ span $V_k(P)$; in particular $V_k(P)$ has dimension less than $k-1$.

Proposition 3.2. *Let $D=m_1P_1+\cdots+m_kP_k-dP_\infty$ be a degree 0 divisor on C with $d\leq g$, $m_i>0$ and $P_i\neq P_j$; then D is reduced if and only if the following matrix*

$$\begin{pmatrix} f_0(P_1) & \cdots & f_{g-1}(P_1) \\ \vdots & \cdots & \vdots \\ (D^{(m_1-1)}f_0)(P_1) & \cdots & (D^{(m_1-1)}f_{g-1})(P_1) \\ \vdots & \cdots & \vdots \\ f_0(P_k) & \cdots & f_{g-1}(P_k) \\ \vdots & \cdots & \vdots \\ (D^{(m_k-1)}f_0)(P_k) & \cdots & (D^{(m_k-1)}f_{g-1})(P_k) \end{pmatrix}$$

has rank d.

Proof: From the discussion preceding the proposition, we see that the points whose homogeneous coordinates are the rows of the matrix above generate the intersection of the hyperplanes in $\mathbb{P}^{g-1}$ whose intersection divisor with $\phi_K(C)$ is $\geq m_1P_1+\cdots+m_kP_k$. From Proposition 1.1 the divisor D is reduced if and only if this intersection has dimension $d-1$, and this is equivalent for the matrix above to have rank d. □

3.4. **Reduction process on C_{ab}-curves.** We now use the results of the preceding sections to give a description of the reduction process for C_{ab}-curves. Assume that we have an affine divisor E (*resp.* E') of degree $g+1$ (*resp.* g) on C; from lemma 1.3, we can find a quadric Q_E such that $Q_E\cdot\phi_K(E)\geq E+(2g-5)P_{K,\infty}$ (*resp.* $Q_E\cdot\phi_K(E)\geq E+(2g-4)P_{K,\infty}$). We first look at the intersection of the canonical model with quadrics, and reinterpret the conditions

$$I_{P_\infty}(Q_E,\phi_K(C))\geq 2g-5 \quad (\textit{resp. } 2g-4).$$

By the lemma 3.2, this just means that the homogeneous equation of the quadric Q contains just monomials X_kX_l such that:

$$\begin{aligned} & I_{P_{K,\infty}}(X_kX_l,\phi_K(C))\geq 2g-5 \quad (\textit{resp. } 2g-4)\\ \Leftrightarrow\ & I_{P_{K,\infty}}(X_k,\phi_K(C))+I_{P_{K,\infty}}(X_l,\phi_K(C))\geq 2g-5 \quad (\textit{resp. } 2g-4)\\ \Leftrightarrow\ & 4g-4-(n_k+n_l)\geq 2g-5 \quad (\textit{resp. } 2g-4)\\ \Leftrightarrow\ & n_k+n_l\leq 2g+1 \quad (\textit{resp. } 2g). \end{aligned}$$

Now the sequel of the reduction process takes place away from $P_{K,\infty}$, and we can use the isomorphism ϕ to come back to the affine plane model. The former condition reduces then (by the isomorphism $\phi^{\#}$) to considering intersections of $\phi_D(C)$ with curves defined by polynomials of the form:

$$\sum_{ij} c_{ij} x^i y^j, \quad ai + bj \leq 2g + 1$$

for the first step, and for the second:

$$\sum_{ij} c_{ij} x^i y^j, \quad ai + bj \leq 2g.$$

Remark 3.1. *In* [4]*, the case of Picard curves is treated; these are nonhyperelliptic curves of genus* 3*, and their canonical model is in* $\mathbb{P}^2$*. In order to reduce degree* 4 *divisors, the authors use interpolating functions. Given* E*, a degree four divisor, the interpolating function* v_E *is just as in the proof of proposition 1.4 above: it is constructed from the quadric* Q_E*. Note that from the discussion above, since here* $2g + 1 = 7$*, the function* v_E *is in* $Vect(1, x, y, x^2, xy)$*.*

In [2]*, the authors discuss the case of trigonal curves of genus* 4*, with a plane equation of the form* $y^3 = p_5(x)$*. They use their canonical model in* $\mathbb{P}^3$ *and the geometric version of Riemann Roch theorem to give a unique representation of the points of* $J_C(k)$ *in terms of affine effective divisors on* C*, then they use interpolating functions to perform reduction in* $\mathrm{Div}^0(C)(k)$*. Again, the quadrics presented here coincide with these interpolating functions.*

Example 3.1. *We end this section with two examples illustrating the above reduction process.*

Let C *be the* C_{43} *curve with plane equation* $y^4 = x^3 + x$*, defined over* $\mathbb{F}_{37}$*; since it has genus* 3*, its canonical model is just the projective closure of this model, with equation* $Y^4 = X^3Z + XZ^3$*. The points* $P_1(17 : 15 : 1)$*,* $P_2(27 : 11 : 1)$*,* $P_3(2 : 10 : 1)$ *and* $P_4(11 : 10 : 1)$ *are in* $C(\mathbb{F}_{37})$*, and the point at infinity is* $P_\infty(1 : 0 : 0)$*. In the sequel we give two degree zero divisors of the form* $D = E - 4P_\infty$*, the equations of the hypersurfaces* Q_E*,* $Q_{E'}$*, and the divisors* E'' *of degree* 3 *such that* $E'' - 3P_\infty$ *is the reduction of* D*:*

i) let $D = P_1 + P_2 + P_3 + P_4 - 4P_\infty$*; the hypersurfaces* Q_E *and* $Q_{E'}$ *have homogeneous equations respectively*

$$Q_E : \ Z^2 + XZ + 32YZ + 11XY + 9Y^2 = 0; \ Q_{E'} : \ 11Z^2 + Y^2 = 0,$$

and we get $E'' = (11 : 27 : 1) + (2 : 27 : 1) + (2 : 10 : 1)$*.*

ii) let $D = P_1 + P_2 + 2P_4 - 4P_\infty$*; the hypersurfaces* Q_E *and* $Q_{E'}$ *have homogeneous equations respectively*

$$Q_E : \ 4Z^2 + 4XZ + 17YZ + 7XY + 36Y^2 = 0; \ Q_{E'} : \ 11Z^2 + Y^2 = 0,$$

and we get $E'' = (11 : 10 : 1) + (2 : 27 : 1) + (11 : 27 : 1)$*.*

References

[1] Arbarello, E., Cornalba, M.,Griffiths, P.A.,Harris, J.: Geometry of algebraic curves, Vol. I, Grundlehren der Mathematischen Wissenschaften, Springer-Verlag, New-York, 1985.

[2] Blache, R., Cherdieu, J.P., Estrada Sarlabous, J.: *Some computational aspects of curves in the family* $y^3 = \gamma x^5 + \delta$ *over* $\mathbb{F}_p$, to appear in Finite Fields and Applications.

[3] Cantor, D.G.: *Computing in the Jacobian of an hyperelliptic curve*, Math. Comp. **48** (1987) pp. 95-101.

[4] Estrada Sarlabous, J., Reinaldo Barreiro E., Piñeiro Barceló, J.A.: *On the Jacobian varieties of Picard curves: explicit addition law and algebraic structure*, Math. Nachr. **208** (1999) pp. 149-166.

[5] Galbraith, S.D., Paulus, S., Smart, N.P.: *Arithmetic on superelliptic curves*, Math. Comp. **71** (2002) n 237 pp. 393-405.

[6] Hartshorne, R.: Algebraic geometry, GTM **52**, Springer-Verlag, New-York, 1977.

[7] Harasawa, R., Suzuki, J.: *Fast Jacobian group arithmetic on* C_{ab} *curves*, in Algorithmic Number Theory (ANTS IV, Leiden, 2000), W. Bosma editor, LNCS **1838** pp. 359-376, Springer, 2000.

[8] Khuri-Makdisi, K.: *Linear algebra algorithms for divisors on an algebraic curve*, Mathematics of Computation **73** pp. 333-357, 2004.

[9] Khuri-Makdisi, K.: *Asymptotically fast group operations on Jacobians of general curves*, preprint avalaible from `http://arxiv.org/abs/math.NT/0409209`.

[10] Milne, J.S.: *Jacobian varieties*, in Arithmetic geometry, G.Cornell and J.Silvermann editors, pp. 167-212, Springer, 1986.

[11] Mumford, D.: *Varieties defined by quadratic equations*, in Questions on algebraic varieties, pp. 29-100, Centro Internazionale Matematica estivo, Cremonese, Roma, 1970 .

[12] Saint Donat, B.: *On Petri's analysis of the linear system of quadrics through a canonical curve*, Math. Ann. **206** (1973) pp. 157-175.

[13] Stöhr, K.-O., Voloch, J.F.: *Weierstrass points and curves over finite fields.*, Proc. London Math. Soc. (3) **52** (1986) pp. 1-19.

Université de Polynésie Française
E-mail address: `blache@upf.pf`

Instituto de Cibernética, Matemática y Física, CITMA, Cuba
E-mail address: `jestrada@icmf.inf.cu`

Humboldt Universität zu Berlin, Germany
E-mail address: `mpetkova@mathematik.hu-berlin.de`