Math. Nachr. (1996),

Decoding of codes on Picard curves

By Jorge Estrada Sarlabous and Jorge Alejandro Piñeiro Barceló

(Received)

Abstract. The Picard curves are genus three curves with a non trivial automorphism, which have been intensively studied due their connection with interesting number theoretic problems.
In 1989, R. Pellikaan obtained an algorithm decoding geometric codes up to $\lfloor (d^* - 1)/2 \rfloor$-errors, where d^* is the designed distance of the code. His algorithm is not completely effective, but recently some authors have given an effective answer to Pellikaan's algorithm using the particular features of special curves, such as the Klein quartic and the hyperelliptic curves.

In this paper we show that the Picard curves are suitable to obtain an effective answer to Pellikaan's algorithm .

1. Introduction and Notations

In 1989, Pellikaan [Pel] presented an algorithm for decoding algrebraic geometry codes that requieres the effective construction of an s-tuple of divisors with some special properties .

In order to be precise, let's fix some notations:

$X/\mathbb{K}$ is a non singular, absolutely irreducible projective curve of genus g, over a field $\mathbb{K}$

$\mathcal{S}_l$ is the set of effective divisors on X with degree l,

$X(\mathbb{K})$ is the set of $\mathbb{K}$-rational points on X,

$J(X)/\mathbb{K}$ is the Jacobian variety of X over $\mathbb{K}$,

$[D]$ is the class of the divisor D in $J(X)$,

$\langle g \rangle$ denotes the intersection divisor of $g = 0$ with X,

If $g = 3$ and X is not hyperelliptic, for any divisor $D \in \mathcal{S}_2$, D' denotes the divisor of $\mathcal{S}_2$, such that $[D'] = [-D]$.

$\mathcal{D} = P_1 + P_2 + ... + P_n \in \mathcal{S}_n$, $P_i \neq P_j, i \neq j$,

1991 *Mathematics Subject Classification.*
Keywords and phrases. Error Correcting Codes, Picard curves, Jacobian Varieties.

$\mathcal{G}$ divisor with $supp(\mathcal{G}) \cap supp(\mathcal{D}) = \emptyset$ and $4g-1 \leq deg(\mathcal{G}) \leq n+2g-2$,
$C = C_\Omega(\mathcal{D},\mathcal{G})$ (the dual code of $C_L(\mathcal{D},\mathcal{G})$) is a $[n,k,d]$ code with $n = deg(\mathcal{D})$, $k = n+g-1-deg(\mathcal{G})$, $d \geq d^* = deg(\mathcal{G})+2-2g$, $t^* = \lfloor (d^*-1)/2 \rfloor$.

$\Psi_w^s : \mathcal{S}_w^s \rightarrow J(X)^{s-1}$ is the mapping defined by $(F_1, F_2, ..., F_s) \rightarrow ([F_1-F_2], [F_2-F_3], ..., [F_{s-1}-F_s])$ with $w = g-2$, if $deg(G)$ is even, $w = g-1$ otherwise.

Applying Skorobogatov and Vladuts basic decoding algorithm [SkV] a number of times in parallel, Pellikaan [Pel] shows :

Theorem 1.1. *Let be $q \geq 3, s \geq 2$, if Ψ_w^s is non surjective and if for some $\mathcal{F} = (F_1, ..., F_s) \in \mathcal{S}_{g+t^*}^s$ $\Psi_{g+t^*}^s(\mathcal{F}) := ([F_1-F_2],[F_2-F_3],...,[F_{s-1}-F_s])$ is not in $Im(\Psi_w^s)$, then exists an algorithm of complexity $O(n^4)$ in time and $O(n^3)$ in space, decoding up to t^*-errors.*

Pellikaan [Pel] and Vladuts [Vla] gave conditions on q and X for the existence of $s \geq 2$, with Ψ_w^s non surjective. The problem is to construct effectively the s-tuple $\mathcal{F}$.

For $g \geq 2$ the effective solution is not trivial and requieres deeper information about the geometry of the curve X.

D. Le Brigand gives an effective answer for a particular hyperelliptic curve as well as a sufficient condition for more general hyperelliptic curves ($X : y^2 + y = p_m(x)$):
" If X is a hyperelliptic curve of genus g defined on $\mathbb{K} = GF(q)$ and if exists a rational and reduced divisor $\mathcal{F} = \sum_{i=1}^{g} R_i - g\infty$, where the coordinates of the points R_i are in $GF(q^g)$, but don't belong to any smaller extension of $\mathbb{K}$, then the map Ψ_{g-1}^2 isn't surjective" (see [LeB]).

D. Rotillon and J.A. Thiong Ly [RoT] give an effective solution for the Klein quartic over F_8, with $deg(\mathcal{G})$ even ($X : x^3y + y^3z + z^3x = 0$).

Several authors have been studying another special family of curves, the Picard curves, due their connection with interesting number theoretical problems, such as the generalization of some Hilbert problems [Hol1], [Hol2],[Hol3],[Holz], [Est1],[Est2].

In this paper we show that the Picard curves may be used to find an effective answer to Pellikaan's algorithm. Moreover, the sufficient conditions on the Picard curves to give a suitable s-tuple of divisors are very easy to check and cover the case $deg(\mathcal{G})$ even as well as the case $deg(\mathcal{G})$ odd.

1.1. Some geometric facts about Picard curves.

Definition 1.2. A Picard curve X/K is a genus three curve attached with a non trivial $\sigma \in Aut_{\overline{\mathbb{K}}}(X)$, such that $\sigma^3 = id_X$ and $(X \otimes_{\mathbb{K}} \overline{\mathbb{K}})/ < \sigma > \cong P^1_{\overline{\mathbb{K}}}$ for some extension $\overline{\mathbb{K}}/\mathbb{K}$.

Theorem 1.3. *If $char(\mathbb{K}) \neq 3$, the Picard curve $X/\mathbb{K}$ is $\overline{\mathbb{K}}$-birrationally equivalent to the non singular, absolutely irreducible curve with projective model:*

$$X_h : zy^3 = a_4x^4 + a_3x^3z + a_2x^2z^2 + a_1xz^3 + a_0z^4 = a_4 \prod (x - \alpha_j z), \tag{1.1}$$

with $\alpha_j, a_j \in \overline{\mathbb{K}}, \alpha_j \neq \alpha_i$ for $i \neq j$.

In these coordinates, σ has the expresion $\sigma(x : y : z) = (x : \xi y : z)$, for ξ solution of $\xi^2 + \xi + 1 = 0$. A proof of theorem 1.3 can be found in [Holz].

A PICARD curve X/F_q has a g_3^1. Let's consider the morphism associated to the g_3^1, $\varphi : X/\overline{F_q} \to P^1_{\overline{F_q}}$, where $\overline{F_q}$ denotes the algebraic closure of F_q .

If $q \equiv 2$ mod 3, in [Est1] is shown that the restriction of φ to X/F_q is $1:1$ onto $P^1_{F_q}$.

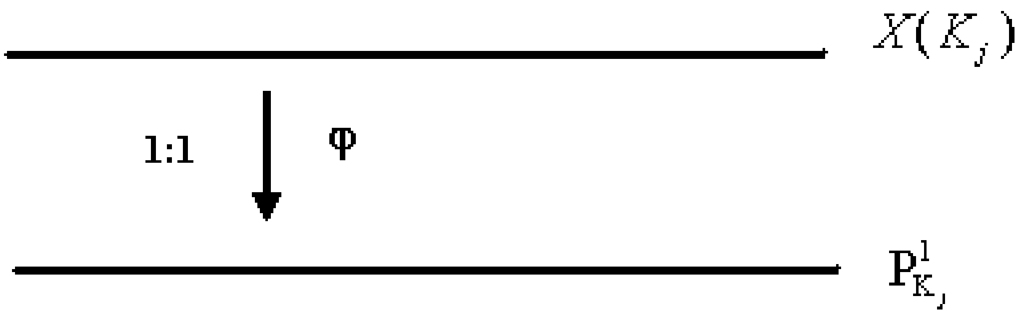

Fig. 1 Case $q^j \equiv 2 \pmod 3$

If $q \equiv 1$ mod 3, the morphism $\varphi : X/\overline{F_q} \to P^1_{\overline{F_q}}$ is a $3:1$ covering, ramified exactly at the point $\infty := (x : y : z) = (0 : 1 : 0)$ and at the points $R_j := (x : y : z) = (\alpha_j : 0 : 1)$, for $j = 1, 2, 3, 4$. All ramification points of φ are total ramification points. If Q is a point different to the φ-images of the ramification points; then $\varphi^{-1}(Q)$ consists of three different points $P, \sigma(P), \sigma^2(P)$, for some point $P \in X/\overline{F_q}$.

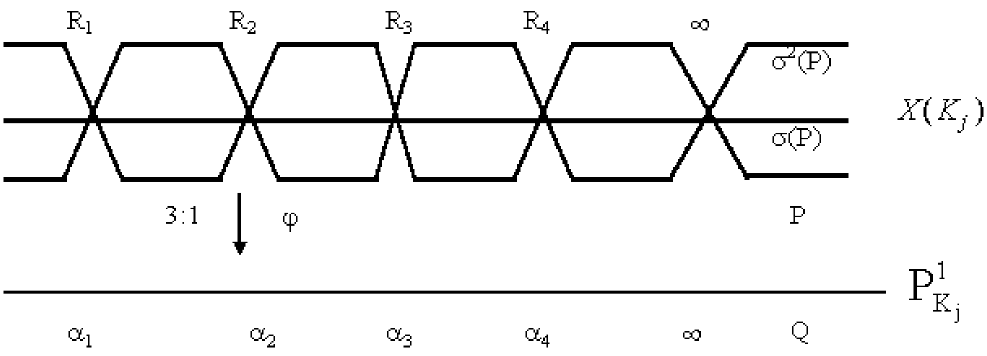

Fig. 2 Case $q^j \equiv 1 \pmod 3$

All ramification points are inflection points of X with inflection tangents $x - \alpha_j z = 0$ at R_j and $z = 0$ at ∞ (the canonical bitangent). Observe that the inflection points R_j are collinear (they belong to the line $y = 0$) and note also that any line passing through two (σ-)conjugate points P and $\sigma(P)$ cuts off X on the remaining conjugate point $\sigma^2(P)$ and on ∞ .

Proposition 1.4. *If X is a* PICARD *curve and two different effective divisors of degree three D_1 and D_2 are equivalent in $J(X)$, then the points of supp(D_j) are collinear for $j = 1, 2$.*

Proof.

The canonical class K of the PICARD curve X is the class of divisors arising from the intersection of straight lines with X, since the differentials $\frac{dx}{y^2}, \frac{x\,dx}{y^2}$ and $\frac{dx}{y}$ form a basis of abelian differentials on X (see [Est1]).

Two different effective divisors of degree three D_1 and D_2 are equivalent in $J(X)$ if and only if $l(D_j)$, the dimension of the linear space $\mathcal{L}(D_j)$ is strictly greater than one, for $j = 1, 2$.

Applying the RIEMANN-ROCH theorem to $D = D_j$ $(deg(D) = genus(X) = 3)$,

$$l(D) = l(K - D) + 1 \qquad (1.2)$$

Let's assume $l(D) > 1$ (i.e. $\mathcal{L}(D) \neq \mathbb{K}$) holds, then $l(K - D) \geq 1$, hence exists a degree 4 effective divisor D'' consisting of 4 collinear points such that $D'' \succeq D$.

On the other hand, if $K \succeq D$ then $K - D$ is an effective divisor, therefore $l(K - D) \geq 1$ and from (1.2) follows $l(D) > 1$.

□

1.2. Non canonical bitangents on PICARD curves.

By definition, a theta characteristic in $char(\mathbb{K}) = 2$ case is a divisor class θ, such that 2θ is the canonical class. If $x \in \mathbb{K}\backslash\mathbb{K}^2$ is a separating variable, the divisor of the exact non zero differential dx is of the form $2D_0$, and the class of D_0 is a theta characteristic and is independent of the selection of x. The class of D_0 is called the canonical theta characteristic.

STÖHR and VOLOCH show in [StV] how to obtain all bitangents l to X from the HASSE-WITT matrix:

- There is a $\frac{1}{2}$-linear bijection from the space of regular exact differentials onto $\mathcal{L}(D_0)$.
- There is a canonical bijection between the set of regular logarithmic non zero differentials and the set of non canonical theta characteristics, sending ω to the class of $\frac{1}{2}div(\omega)$.
- Each non canonical theta characteristic is represented by a positive divisor. If the HASSE-WITT matrix has $rank < genus(X)$, it also holds true for the canonical theta characteristic.
- If $genus(X) = 3$ and X is non hyperelliptic, identifying X with its canonical curve, the set of positive divisors which represent theta characteristics correspond bijectively to the bitangents of X. If $H = (h_{i,j})$ is the HASSE-WITT matrix with respect to the adjoint polynomials $1, x, y$, the non canonical bitangents are given by the equations $l : c_1 + c_2x + c_3y = 0$ with c_j satisfying the conditions $\sum_{i=1}^{3} c_i h_{i,j} = c_j^2$, for $j = 1, 2, 3$ and c_j not all simultaneously equal to zero.

In [Est1], the HASSE-WITT matrix of PICARD curves are computed. In the case we are dealing with $(char(K) = 2)$, the HASSE-WITT matrix H is:

$$H = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ a_1 & a_3 & 0 \end{pmatrix}, \text{ for } X_h \text{ the projective model in 1.1 and } \mathbb{K} = F_q.$$

Hence, the non canonical bitangents l on X are:

$$\begin{cases} l : c_1 + c_2x + c_3y = 0, & (c_j) \neq (0, 0, 0), \\ \qquad a_1c_3 = c_1^2, & a_3c_3 = c_2^2, \qquad c_2 = c_3^2 \end{cases}$$

- Case $a_1 \neq 0$.
  $l_j : a_1^2\xi^j + \eta^3\xi^j x + \eta\xi^{2j}a_1 y = 0$, $j = 0, 1, 2$
  $\xi^2 + \xi + 1 = 0$, $\eta^6 = a_3a_1^3$, $\eta \in F_q$.
  l_j cutts off X at the points $(x : y : z) = (x_i : y_i : 1)$, where x_i is a solution of $x^2 + \sqrt{\frac{a_2a_1+\eta^3}{a_1}}x + \sqrt{\frac{a_0\eta^3+a_1^3}{\eta^3}} = 0$, and $y_i = \xi^{-j}\left(\frac{a_1^2+\eta^3x_i}{\eta a_1}\right)$.

- Case $a_1 = 0$.
  $l_j : \eta\xi^j x + y = 0$, $j = 0, 1, 2$
  $\xi^2 + \xi + 1 = 0$, $\eta^3 = a_3$, $\eta \in F_q$
  l_j cutts off X at the points $(x : y : z) = (x_i : y_i : 1)$, where x_i is a solution of $x^2 + \sqrt{a_2}x + \sqrt{a_0} = 0$, and $y_i = \xi^j \eta x_i$.

Once we have computed all non canonical bitangents to a PICARD curve, it is easy to check that they cut off X on points on $X(F_{q^2})$.

2. Effective sufficient conditions for PELLIKAAN'S algorithm.

Let X be a non hyperelliptic PICARD curve with projective model X_h defined over F_q, $q = 2^j$, $q \equiv 2 \bmod 3$ and set:

- $\mathcal{D} := \sum P_j + \sigma(P_j) + \sigma^2(P_j)$, for all $P_j \in X(F_{q^3}) \backslash X(F_q)$, $P_i \neq P_j$ for $i \neq j$
- $\mathcal{G} := mQ$ for $Q := \sum Q_j + \sigma(Q_j) + \sigma^2(Q_j)$, Q_j running over all points of $X(F_q)$, $Q_j \neq Q_i$, for $j \neq i$, m suitably choosen, such that $4g - 1 \leq deg(\mathcal{G}) \leq deg(\mathcal{D}) + 2g - 2$ (recall $deg(\mathcal{G}) = 3m(1 + q)$).

Then by construction the supports of $\mathcal{D}$ and $\mathcal{G}$ are disjoint. $C = C_\Omega(\mathcal{D}, \mathcal{G})$ (the dual code of $C_L(\mathcal{D}, \mathcal{G})$) is a $[n, k, d]$ code with $n = deg(\mathcal{D}) = 3q(q^2 - 1)$, $k = n + g - 1 - deg(\mathcal{G}) = 3q(q^2 - 1) - 3m(1 + q) + 2$, $d \geq d^* = 3m(1 + q) - 4$.

The code $C = C_\Omega(\mathcal{D}, \mathcal{G})$ is a lifting of the BCH code defined by the pair of disjoint divisors on the projective line $\varphi(\mathcal{D})$ and $\varphi(\mathcal{G})$ (compare with the hyperelliptic case in [ReT]).

2.1. Case $\deg(\mathcal{G})$ even (ie. $w = g - 2 = 1$)

Proposition 2.1. *Let $P \in X(F_{q^2})$, such that X has a non canonical bitangent at P. Then it is possible to construct a pair $(F_1, F_2) \in \mathcal{S}^2_{g+t^*}$, such that the supports of $\mathcal{D}$ and F_i are disjoint for $i = 1, 2$ and $[F_1 - F_2]$ is not in the image of Ψ^2_1.*

Proof. If $P \neq \infty$ and X has a bitangent at P, then X has also non canonical bitangents l_j at the conjugate points $\sigma^j(\mathrm{P})$, for $j = 0, 1, 2$. Note that $l_j \cap l_r \cap X = \emptyset$, for $j \neq r \bmod 3$. Set:

$F_j = 2\sigma^j(P) + (g + t^* - 2)P$, for $j = 1, 2$.

If $(H_1, H_2) \in \mathcal{S}^2_1$ and $[H_1 - H_2] = [F_1 - F_2]$, then $\left[H_1 + 2\sigma^2(P)\right] = [H_2 + 2\sigma(P)]$.
After the proposition 1.4, two divisors of $\mathcal{S}_3$ are equivalent in $J(X)$ if and only if they coincide or each consists of three collinear points .

- If $H_1 + 2\sigma^2(P) = H_2 + 2\sigma(P)$, then $H_1 = \sigma(P)$ and $H_2 = \sigma^2(P)$, hence $\sigma(P) = \sigma^2(P)$, i.e., P is a ramification point at which X has a bitangent. Hence $P = \infty$, a contradiction!.
- If $H_1 + 2\sigma^2(P) \neq H_2 + 2\sigma(P)$ but $\left[H_1 + 2\sigma^2(P)\right] = \left[H_2 + 2\sigma(P)\right]$, then from the collinearity of the points of each divisor follows $H_1 = \sigma^2(Q)$ and $H_2 = \sigma(Q)$, for Q equal to the remaining intersection point of the bitangent at P with X. Since $\left[2\sigma^j(P) + 2\sigma^j(Q) - 4\infty\right] = 0$ it follows:

$$\begin{array}{ccc} \left[\sigma^2(Q) + 2\sigma^2(P)\right] & = & \left[\sigma(Q) + 2\sigma(P)\right] \\ \left[(\sigma^2(Q) + 2\sigma^2(P)) + \sigma^2(Q) + \sigma(Q)\right] & = & \left[(\sigma(Q) + 2\sigma(P)) + \sigma^2(Q) + \sigma(Q)\right] \\ \left[\sigma(Q)\right] & = & \left[\sigma^2(Q)\right] \end{array}$$

If $Q \neq \infty$ (otherwise follows $P = \infty$), from $[\sigma(Q)] = \left[\sigma^2(Q)\right]$ we get

$$[2\sigma(Q) + Q] = \left[\sigma^2(Q) + \sigma(Q) + Q\right] = [3\infty]$$

hence from Prop. 1.4, Q is a ramification point, a contradiction again! .

□

2.2. Case deg($\mathcal{G}$) odd (ie. w = g-1 = 2).

Proposition 2.2. *If $p_4(x) = \sum a_j x^j$ has no roots in $F_{q^3} \backslash F_q$, then it is possible to construct a 4-tuple $(F_1, F_2, F_3, F_4) \in \mathcal{S}^4_{g+t^*}$, such that supp($F_i$)$\cap$ supp($\mathcal{D}$) $= \emptyset$ and $([F_1 - F_2], [F_2 - F_3]\ , [F_3 - F_4]) \notin Im(\Psi_2^4)$.*

Proof. With the above hypothesis on $p_4(x)$, the ramification points R_j are not contained in *supp*($\mathcal{D}$), for $j = 1, 2, 3, 4$. Take, as before, $P \in X(F_{q^2})$ such that X has a non canonical bitangent at P and set:

$$\begin{array}{lcl} F_1 & := & (g + t^*)\infty, \\ F_2 & := & R_4 + (g + t^* - 1)\infty, \\ F_3 & := & R_3 + R_4 + (g + t^* - 2)\infty, \\ F_4 & := & 2R_3 + 2R_4 + \sigma(P) + \sigma^2(P) + (g + t^* - 6)\infty. \end{array}$$

Then *supp*(F_j) $\cap$ *supp*($\mathcal{D}$) $= \emptyset$, for $j = 1, 2, 3, 4$. We are going to use the following fact:

Lemma 2.3. *Let be $H_1, H_2, H_3, H_4 \in \mathcal{S}_2$, such that $[H_1 - H_2] = [R_1 + R_2 + R_3 - 3\infty]$, $[H_3 - H_2] = [R_1 + R_2 + R_4 - 3\infty]$. Then, there are only five possibilities for H_3: $H_3 = R_1 + \infty, H_3 = R_2 + \infty, H_3 = R_1 + R_2, H_3 = 2R_3$ or $H_3 = 2\infty$.*

Proof.
From the fact $[H_2 - H_1] = [R_1 + R_2 + R_3 - 3\infty]$ follows

$$H_1 - H_2 + R_1 + R_2 + R_3 - 3\infty \sim 0$$

and from this we have

$$R_1 + R_2 + R_3 + \infty + H_1 + H_2' - 8\infty = < g >$$

for some quadric g.
As $< y > \succeq R_1 + R_2 + R_3$ and $\infty \cap supp(< y >_0) = \emptyset$ after Bezout's Theorem $< g > = (y.(x - x_0))$ holds, for some $x_0 \in \overline{\mathbb{K}}$. Hence, $H_1 + H_2 = R_4 + P_0 + \sigma(P_0) + \sigma^2(P_0)$ with $P_0 = (x_0, y_0) \in X$. This lead us essentially to two cases (either H_1 or H_2' consists of two conjugate points):

- $H_2' = R_4 + P_0$, $H_1 = \sigma(P_0) + \sigma^2(P_0)$

$$H_2 - H_3 + R_1 + R_2 + R_4 - 3\infty \sim 0$$
$$H_2 + H_3' + R_1 + R_2 + R_4 - 7\infty \sim 0$$
$$H_3' - H_2' + R_1 + R_2 + R_4 - 3\infty \sim 0$$
$$H_3' - P_0 + R_1 + R_2 - 3\infty \sim 0$$

  therefore $R_1 + R_2 + \sigma(P_0) + \sigma^2(P_0) + H_3' - 6\infty = < q >$, for some quadric q.
  If $P_0 = \infty$, then $H_3' = R_3 + R_4$, hence $H_3 = R_1 + R_2$.
  If $P_0 \neq \infty$, then $q = (x - \alpha_1)(x - \alpha_2)$, so follows $H_3' = 2R_2$ and $H_3 = R_1 + \infty$ or $H_3 = R_2 + \infty$.

- $H_1 = R_4 + P_0$, $H_2' = \sigma(P_0) + \sigma^2(P_0)$
  Then $H_2 = \infty + P_0$ and $R_1 + R_2 + R_4 + \infty + H_3' + P_0 + \infty - 8\infty \sim 0$, but

$$-(R_1 + R_2 + R_4 + P_0 + \infty) + 8\infty \sim R_3 + \sigma(P_0) + \sigma^2(P_0)$$

  Therefore, $R_3 + \sigma(P_0) + \sigma^2(P_0) \sim H_3' + \infty$
  If $R_3 + \sigma(P_0) + \sigma^2(P_0) = H_3' + \infty$, then $P_0 = \infty$ hence, $H_3' = \infty + R_3$ and $H_3 = 2R_3$.
  If $R_3 + \sigma(P_0) + \sigma^2(P_0) \neq H_3' + \infty$, there exists by Prop. 1.4 a line r such that $< r > \succeq R_3 + \sigma(P_0) + \sigma^2(P_0)$, hence $P_0 = R_3$, $H_3' = 2\infty$ and $H_3 = 2\infty$.

□

If we assume the existence of $H_1, H_2, H_3, H_4 \in \mathcal{S}_2$, such that $[H_2 - H_1] = [F_1 - F_2] = [R_1 + R_2 + R_3 - 3\infty]$ and $[H_3 - H_2] = [F_2 - F_3] = [R_1 + R_2 + R_4 - 3\infty]$, then by the lemma 2.3 there are only five possibilities for H_3.

If furthermore holds $[H_4 - H_3] = [F_3 - F_4] = [R_3 + R_4 + P - 3\infty]$, then exists a quadric q interpolating X at the divisor $\infty + H_3 + H_4$. By repeated use of the Prop. 1.4 and the collinearity of the affine ramification points R_j, for any possible H_3 we obtain that $P \in \{\infty, R_1, R_2, R_3, R_4\}$, a contradiction!

Let's consider, for example, the case $H_3 = \infty + R_1$
$< q >= \infty + R_1 + R_1 + R_2 + P + \infty + H_4' - 8\infty \sim 0$. On the other hand,

$$\infty + R_1 + R_1 + R_2 + P + R_1 + (R_2 + P)' \sim 8\infty$$

hence $\infty + H_4' \sim R_1 + (R_2 + P)'$, therefore $R_1 + H_4 \sim \infty + R_2 + P$
If $R_1 + H_4 = \infty + R_2 + P$, then $P = R_1$. Otherwise, by Prop 1.4, $P = R_2$.
All remaining cases for H_3 may be prooved by similar arguments. □

3. Numerical examples.

The polynomials $p_4(x) = x^4+x^3+x^2+x+1$ and $\overline{p_4}(x) = x^4+x^3+1$ are F_q-irreducible for $q = 2^k, q \equiv 2 \bmod 3$.

The PICARD curves X_h: $zy^3 = z^4 p_4(x/z)$ and $\overline{X_h}$: $zy^3 = z^4\overline{p_4}(x/z)$ are defined over F_q, non singular and non hyperelliptic.

Either if $deg(G)$ is even or odd, denoting as P the point at which the curve has a non canonical bitangent, we may take $P := (0 : 1 : 1)$ for X_h and for $\overline{X_h}$ we can take $P := (1 : 1 : 1)$.

Acknowledgements

We wish to thank G. LACHAUD, T. HOHOLDT , C. MORENO, C. RENTERIA *and* H. TAPIA-RECILLAS *for their valuable comments, discussions and encouragement.*
The results contained in this paper were partially obtained during a research stay at IPN/Mexico, which was possible thanks a TWAS South-South Fellowship.
Finally we wish to express our gratitude to the Organizing Committe for the kind invitation to participate at the FWI Mathematical Colloquium, Guadeloupe 1996, in particular to J.-P. CHERDIEU *and* J.-C. MADO *for their warm hospitality.*

References

[LeB] LE BRIGAND, D.: Decoding codes on hyperelliptic curves, Springer LNCS, vol. 514 (1991).

[Est1] ESTRADA-SARLABOUS, J.: On the Jacobian varieties of PICARD curves defined over fields of characteristic ¿ 0, Math. Nachrichten 132, (1991).

[Est2] ESTRADA-SARLABOUS, J., PIÑEIRO, A. and REYNALDO, E.: On the Jacobian Varieties of PICARD curves: Explicit Addition Law and Structure of Abelian Variety, submited to Math. Nachrichten (1996).

[Holz] ESTRADA-SARLABOUS, J.: A finiteness theorem for PICARD curves with good reduction, in "The Ball and some HILBERT Problems" by R.-P. HOLZAPFEL, Birkhäuser-Verlag, (1995).

[Hol1] HOLZAPFEL, R.-P., Geometry and arithmetic around Euler partial differential equations. Dt. Verl. d. Wiss., Berlin/Reidel Publ. Comp., Dordrecht (1986).

[Hol2] HOLZAPFEL, R.-P., On algebraic values of the PICARD modular function. Proc. Special Diff. Equations, Arkata (1991).

[Hol3] HOLZAPFEL, R.-P., Transcendental Ball Points of Algebraic PICARD Integrals. Math. Nachr. 162 (1993).

[Pel] PELLIKAAN, R.: On a decoding algorithm for codes on maximal curves, IEEE Trans. Info. Theory, vol.35, 6 (1989), 1228-1232.

[ReT] RENTERIA, C. and TAPIA-RECILLAS, H.: A Hyperelliptic code which is a lifting of a BCH code, in "The Marshall Hall Conference", D. JUNGNICKEL and S.A. VANSTONE, Eds., J. Wiley & Sons Inc., (1993).

[RoT] ROTILLON, D. and THIONG LY, J.-A.: Decoding of codes on the KLEIN quartic, Springer LNCS, vol. 514, (1991).

[SkV] SKOROBOGATOV, A.N. and VLADUTS, S.G.: On the Decoding of Algebraic-Geometric Codes, IEEE Trans. Info. Theory, vol. 36, 5 (1990), 1051-1060.

[StV] STÖHR K.-O. and VOLOCH , J.: A formula for the CARTIER operator on plane algebraic curves, J. Reine Angewandte Math. 377, (1988).

[Vla] VLADUTS, S.G.: On the decoding of Algebraic-Geometric Codes over F_q, for $q \geq 16$, IEEE trans. Info. Theory, vol. 36, 6 (1990), 1461-1463.

Department of Geometry and Combinatorics.
ICIMAF. Ministry of Sciences.
Calle E No.309, esquina a 15
Vedado 4, C. Habana. Cuba.
E-mail: matdis@cidet.icmf.edu.cu