ELSEVIER Journal of Pure and Applied Algebra 112 (1996) 13–28

JOURNAL OF
PURE AND
APPLIED ALGEBRA

The Theta divisor of a jacobian variety and the decoding of geometric Goppa Codes

Thierry Henocq*, Denis Rotillon

Laboratoire d'Algèbre, UFR MIG, Université Paul Sabatier, 31062 Toulouse, France

Communicated by M.-F. Roy; received 7 November 1993; revised 1 June 1994

Abstract

Pellikaan (1989) has given a noneffective maximal decoding algorithm of a geometric code. To this end, our purpose is the determination of the minimal integer s, such that the maps Ψ^s_{g-k} $(k = 1, 2)$, defined in Pellikaan (1989), are surjective. Then, on the one hand, we show that the theta divisor of the jacobian variety of an algebraic curve provides partial answers. On the other hand, for the Klein quartic defined over $\mathbb{F}_8$, we determine explicitly divisors of degree 8 which allows us to decode up to 5 errors.

1. Introduction

Let χ be an algebraic projective curve, absolutely irreducible, nonsingular, of genus g, $(g \geq 2)$, defined over the finite field $\mathbb{F}_q$ with q elements, where q is a power of a prime integer.

We denote by $\mathrm{Div}(\chi)$ the abelian group of the divisors on the curve χ and by $\mathrm{Pic}^0(\chi)$ the group $\mathrm{Div}(\chi)$ modulo the principal divisors made up of the divisors of degree zero.

It is known [11] that there exists an abelian variety $J(\chi)$ of dimension g and an injective map $\varphi : \chi \to J(\chi)$ such that the extension of χ to $\mathrm{Div}(\chi)$ establishes an isomorphism between $\mathrm{Pic}^0(\chi)$ and $J(\chi)$. Moreover, if O is a rational point of χ over $\mathbb{F}_q$, then φ can be defined by

$$\varphi : \chi \to J(\chi)$$
$$P \mapsto \varphi(P) = [P - O],$$

where $[P - O]$ designates the class of the degree zero divisor $P - O$ in $\mathrm{Pic}^0(\chi)$.

* Corresponding author. E-mail:henocq@cict.fr.

SSDI 0022-4049(95)00008-9

We denote by $\mathbb{D}_r(\chi)$ the effective divisors of degree r of the curve χ and by φ_r the extension of φ to $\mathbb{D}_r(\chi)$

$$\varphi_r : \mathbb{D}_r(\chi) \to J(\chi)$$

$$D \mapsto \varphi_r(P) = [D - r \cdot O].$$

The direct image of φ_r is a sub-variety $\mathbb{W}_r$ of dimension r if $0 \le r \le g$, and of dimension g if not. In particular, $\mathbb{W}_{g-1}$ defines a divisor on $J(\chi)$ called Theta and denoted Θ. If $J(\chi)$ is defined over $\mathbb{F}_q$, then the same holds for Θ together with all its translate spaces [11, Theorem 4, p. 99].

Here, we investigate the maps

$$\Psi^s_{g-k} : \mathbb{D}^s_{g-k}(\chi) \to J^{s-1}(\chi)$$

$$(D_1, \dots, D_s) \mapsto ([D_2 - D_1], \dots, [D_s - D_{s-1}]).$$

More precisely, following [13], first of all we set out to determine over $\mathbb{F}_q$, the minimum exponent integer s, if there any, such that Ψ^s_{g-k} is not surjective ($s \in \mathbb{N}^*$, $k = 1, 2$). Over the algebraic closure of $\mathbb{F}_q$, $\overline{\mathbb{F}}_q$, these maps are not surjective as far as s is large enough. Then, for the purpose of decoding, whenever an algebraic-geometric code is defined on χ with designed minimum distance d^* we look for divisors F_i, $i \in \{1, \dots, s\}$ of degree $g + \lfloor (d^* - 1)/2 \rfloor$ such that the $(s-1)$-uple of $J^{s-1}(\chi)$ represented by

$$([F_2 - F_1], \dots, [F_s - F_{s-1}])$$

has no inverse image through Ψ^s_{g-k}.

In the case of the Klein quartic defined over $\mathbb{F}_8$, for a given code with designed minimum distance 11, we show that $s = 3$ fulfills the first condition above and we determine explicitly a suitable 3-uple of divisors of degree $g + \lfloor (d^* - 1)/2 \rfloor = 8$.

Our approach here is a concrete one, based on the inspection of the linear series on the curve χ; it is used for the first time as far as we known, so as to bring a touch of some effectiveness to the Pellikaan algorithm, which seemed to be lacking at first sight. Needless to say the more recent decoding algorithm such as those from Feng and Rao [6], Duursma [2, 3] and Ehrhardt [4, 5] are admittedly more performing in particular as far as complexity is concerned.

2. The map Ψ^s_{g-1}

Lemma 2.1. *Let Θ^s defined as the self-intersection number of s copies of the divisor Θ. Over $\overline{\mathbb{F}}_q$ we have*

$$\Theta^s \neq 0 \iff \forall (a_1, \dots, a_s) \in J^s(\chi),\ \Theta_{a_1} \cap \Theta_{a_2} \cap \cdots \cap \Theta_{a_s} \neq \emptyset,$$

where $\Theta_{a_i} = \{t + a_i \mid t \in \Theta\}$.

Proof. We know that there exists s translate spaces $\Theta_{a_1}, \Theta_{a_2}, \ldots, \Theta_{a_s}$ such that $\Theta_{a_1} \cap \Theta_{a_2} \cap \cdots \cap \Theta_{a_s}$ is well defined [12]. Moreover, for all other translates, Θ_{b_1}, $\Theta_{b_2}, \ldots, \Theta_{b_s}$, we have

$$\dim(\Theta_{b_1} \cap \Theta_{b_2} \cap \cdots \cap \Theta_{b_s}) \geq \dim(\Theta_{a_1} \cap \Theta_{a_2} \cap \cdots \cap \Theta_{a_s})$$

with an equality in the case when $\Theta_{b_1} \cap \Theta_{b_2} \cap \cdots \cap \Theta_{b_s}$ is well defined. Hence the lemma follows immediately. □

Theorem 2.2. *Over $\overline{\mathbb{F}}_q$, Ψ^s_{g-1} is surjective if and only if $\Theta^s \neq 0$.*

Proof. Obviously, Ψ^s_{g-1} is surjective if and only if

$$\forall (E_1, E_2, \ldots, E_{s-1}) \in J^{s-1}(\chi), \exists (D_1, D_2, \ldots, D_s) \in \mathbb{D}^s_{g-1}(\chi)$$

$$\text{such that } \forall\, i \in \{1, \ldots, s-1\},\ \varphi_{g-1}(D_s) = \varepsilon_{s-i} + \varphi_{g-1}(D_{s-i}) \tag{1}$$

$$\text{with } \varepsilon_i = \textstyle\sum_{k=i}^{s-1} E_k.$$

In addition to that, from Lemma 2.1,

$$\Theta^s \neq 0 \Leftrightarrow \forall (E_1, \ldots, E_{s-1}) \in J^{s-1}(\chi), \exists \xi \in \Theta \cap \Theta_{\varepsilon_1} \cap \Theta_{\varepsilon_2} \cap \cdots \cap \Theta_{\varepsilon as-1}.$$

In view of $\Theta = \mathbb{W}_{g-1}$, $\Theta^s \neq 0 \Leftrightarrow \forall (E_1, \ldots, E_{s-1}) \in J^{s-1}(\chi)$, $\exists (D_1, \ldots, D_s) \in \mathbb{D}^s_{g-1}(\chi)$, $\exists \xi \in J(\chi)$ such that $\forall i \in \{1, \ldots, s-1\}$, $\xi = \varphi_{g-1}(D_s) = \varepsilon_{s-i} + \varphi_{g-1}(D_{s-i})$.

Hence, from (1), the theorem is established. □

Corollary 2.3. *Over $\overline{\mathbb{F}}_q$, Ψ^s_{g-1} is surjective whereas Ψ^{g+1}_{g-1} is not.*

Proof. Over an algebraically closed field, it is known that $\Theta^g = g!$ Thus, $\Theta^g \neq 0$ and $\Theta^{g+1} = 0$ and we are done. □

Remark. Over $\mathbb{F}_q$, it was already known that Ψ^{g+1}_{g-1} was not surjective. Actually, by [13],

$$\dim_{\overline{\mathbb{F}}_q}(\mathbb{D}^{g+1}_{g-1}(\chi)) < \dim_{\overline{\mathbb{F}}_q}(J^g(\chi)).$$

Comments. (1) Vladut [16] has produced curves such that over $\mathbb{F}_2$, $\mathbb{F}_3$ and $\mathbb{F}_4$, Ψ^s_{g-1} is surjective for every $s \in \mathbb{N}^*$.

He has also showed that for any curve considered over $\mathbb{F}_q$, with $q \geq 37$ or, $q \geq 16$ and g large enough, Ψ^{2g}_{g-1} is not surjective [16].

(2) Carbonne and Thiong-Ly [1] have shown that the curves whose zeta-function over $\mathbb{F}_q$ have numerator of the form

$$P(T) = (1 - \sqrt{q} \cdot T)^{2g}$$

satisfy

$$\# \mathbb{D}^g_{g-1}(\chi) < \# J^{g-1}(\chi)$$

and consequently Ψ^g_{g-1} is not surjective in this case, which gives a strictly smaller value for s than in the case over $\overline{\mathbb{F}}_q$.

(3) At last, we prove in the sequel that in the case of the Klein quartic defined over $\mathbb{F}_8$, Ψ^g_{g-1} is not surjective and so the value found for s comes again smaller than the one found over $\overline{\mathbb{F}}_q$, as well as the one found over $\mathbb{F}_q$ by means of the zeta-function.

3. The map Ψ^s_{g-2}

Theorem 3.1. *Over* $\overline{\mathbb{F}}_q$, *if* $\Theta^{2s} \neq 0$ *then* Ψ^s_{g-2} *is surjective.*

Proof. We have Ψ^s_{g-2} is surjective if and only if

$$\forall (E_1, E_2, \ldots, E_{s-1}) \in J^{s-1}(\chi),\ \exists (D_1, D_2, \ldots, D_s) \in \mathbb{D}^s_{g-1}(\chi)$$

$$\text{such that } \forall\ i \in \{1, \ldots, s-1\},\ \varphi_{g-2}(D_s) = \varepsilon_{s-i} + \varphi_{g-1}(D_{s-i}) \tag{2}$$

$$\text{with } \varepsilon_i = \textstyle\sum_{k=i}^{s-1} E_k.$$

Furthermore, by Lemma 2.1,

$$\text{if } \Theta^{2s} \neq 0 \text{ then } \forall (E_1, \ldots, E_{s-1}) \in J^{s-1}(\chi), \exists \xi \in \Theta \cap \Theta^2_{\varepsilon_1} \cdots \cap \Theta^2_{\varepsilon a_s\ 1}.$$

The Poincaré formula, $\Theta^{g-d}/(g-d) \approx \mathbb{W}_d$ holds over an algebraically closed field, where $\approx$ stands for the algebraic equivalence of divisors [13]. In particular, $\Theta^2 \approx 2 \cdot \mathbb{W}_{g-2}$. Thus, if $\Theta^s \neq 0$ then $\forall (E_1, \ldots, E_{s-1}) \in J^{s-1}(\chi)$, $\exists (D_1, \ldots, D_s) \in \mathbb{D}^s_{g-1}$, $\exists \xi \in J(\chi)$ such that $\forall i \in \{1, \ldots, s-1\}$, $\xi = 2\varphi_{g-2}(D_s) = 2\varepsilon_{s-i} + 2\varphi_{g-2}(D_{s-i})$.

Hence the theorem follows from (2). □

Theorem 3.2. *Over* $\overline{\mathbb{F}}_q$, $\Psi^{\lfloor g/2 \rfloor}_{g-2}$ *is surjective whereas* $\Psi^{\lfloor g/2 \rfloor + 1}_{g-2}$ *is not.*

Proof. While

$$\dim_{\overline{\mathbb{F}}_q}(\mathbb{D}^s_{g-2})(\chi)) = (g-2) \cdot s \quad \text{and} \quad \dim_{\overline{\mathbb{F}}_q}(J^{s-1}(\chi)) = g \cdot (s-1),$$

we have, as soon as $s > g/2$,

$$\dim_{\overline{\mathbb{F}}_q}(\mathbb{D}^s_{g-2})(\chi)) < \dim_{\overline{\mathbb{F}}_q}(J^{s-1}(\chi)).$$

Thus $\Psi^{\lfloor g/2 \rfloor + 1}_{g-2}$ is not surjective.

$\Theta^g = g!$ hence $\Theta^{2\lfloor g/2 \rfloor} \neq 0$ and $\Psi^{\lfloor g/2 \rfloor}_{g-2}$ is surjective. □

Corollary 3.3. *Over* $\overline{\mathbb{F}}_q$, Ψ^s_{g-2} *is surjective if and only if* $\Theta^{2s} \neq 0$.

Proof. It is a consequence of Theorems 3.1 and 3.2, of $\Theta^g = g!$ and of $\Theta^2 \approx 2 \cdot \mathbb{W}_{g-2}$. □

Comments. Carbonne and Thiong-Ly [1], have shown that the curves whose zeta-function have numerator over $\mathbb{F}_q$ of the form

$$P(T) = (1 - \sqrt{q}\cdot T)^{2g}$$

satisfy

$$\sharp\mathbb{D}_{g-2}^{\lfloor (g-1)/2\rfloor+1}(\chi) < \sharp J^{\lfloor (g-1)/2\rfloor+1}(\chi),$$

consequently $\Psi_{g-2}^{\lfloor g/2\rfloor-1}$ is not surjective in this case. In particular, when g is odd, $\Psi_{g-2}^{\lceil g/2\rceil}$ is not surjective which gives a strictly smaller value for s than in the case over $\bar{\mathbb{F}}_q$.

Theorem 3.4. *For all curves defined over $\mathbb{F}_q$, with $q \geq 37$ or $q \geq 16$ and g large enough,*

$$a_{g-2} < h\frac{q+3}{2.q\cdot(q-1)}$$

with $h = \sharp J(\chi)$ and $a_{g-2} = \sharp\mathbb{D}_{g+2}(\chi)$. So Ψ_{g-2}^{g} is not surjective.

Proof. We use here the same notations as in [13, Part 3]:

$$a_{g-2} = \sum_{i+j=g-2}\frac{a^{i+1}-1}{q-1}p_j = \frac{1}{q-1}\sum_{j=0}^{g-2}(q^{g-1-j}p_j - p_j).$$

In view of $p_{g+i}/q^i = p_{g-i}$ for $i \in \{1,\dots,g\}$

$$a_{g-2} = \frac{1}{q-1}\sum_{j=0}^{g-2}\left(\frac{p_{2g-j}}{q} - p_j\right) = \frac{1}{q-1}\left[\frac{1}{q}\left(\sum_{j=0}^{2g}p_j - \sum_{j=0}^{g+1}p_j\right) - \sum_{j=0}^{g-2}p_j\right].$$

Since $h = \sum_{j=0}^{g-2}p_j$,

$$a_{g-2} = \frac{1}{q-1}\left[\frac{1}{q}h - \frac{q+1}{q}\sum_{j=0}^{g-2}p_j - \frac{1}{q}(p_{g-1} + p_g + qp_{g+1})\right].$$

Passing to the modulus,

$$a_{g-2} \leq \frac{1}{q-1}\left[\frac{1}{q}h - \frac{q+1}{q}\sum_{j=0}^{g-2}|p_j| + \frac{q+1}{q}|p_{g-1}| + \frac{|p_g|}{q}\right],$$

so

$$a_{g-2} \leq \frac{1}{q(q-1)}\left[h + (q+1)\sum_{j=0}^{g}|p_j|\right].$$

For $j \in \{1,\dots,2g\}$, $|p_j| \leq C_{2g}^{j}q^{j/2}$. Then

$$a_{g-2} \leq \frac{1}{q(q-1)}\left[h + (q+1)\sum_{j=0}^{g}C_{2g}^{j}q^{j/2}\right].$$

From the Newton formula it yields that

$$a_{g-2} \leq \frac{1}{q(q-1)}\left[h + (q+1)\, q^{g-2}\, 2^{2g-1}\right].$$

Firstly from [13],

$$h \geq (q^{1/2}-1)^{2g},$$

hence,

$$\frac{a_{g-2}}{h} \leq \frac{1}{q(q-1)}\left[1 + \frac{(q+1)}{2}\left(\frac{4q^{1/2}}{(q^{1/2}-1)^2}\right)^g\right].$$

Secondly from [16],

$$h \geq \frac{(4q^{1/2})^g}{f_q(g)}$$

with

$$f_q(g) = \max\{1,b\}\,(4q^{-1/2})^g\, q^{1+2gq[(b+1)(q-1)]}\left(\frac{q-1}{q}\right)^{N_1(g-1)/g}$$

hence

$$\frac{a_{g-2}}{h} \leq \frac{1}{q(q-1)}\left[1 + \frac{(q+1)}{2} f_q(g)\right].$$

Again by [16], we know that for $q \geq 37$, $[(4q^{1/2}/(q^{1/2}-1)^2)^g] < 1$ or that for $q \geq 16$, $f_q(g)$ tends to 0 for $g \to \infty$. We can conclude. □

4. Explicit search for divisors establishing the nonsurjectivity of Ψ^g_{g-1} for the Klein quartic over $\mathbb{F}_8$

We are concerned with the Klein quartic $\mathscr{K}$, whose equation is

$$X^3Y + Y^3Z + Z^3X = 0.$$

We work over the field $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$, where α is root of the primitive polynomial $X^3 + X + 1 = 0$.

$\mathscr{K}$ is nonsingular of genus 3. Let $\mathscr{K}(\mathbb{F}_8)$ be the set of the 24 rational points P_i, $i \in \{1,\dots,24\}$, over $\mathbb{F}_8$ which attains the Serre upper bound.

Its canonical linear serie K is the unique g_4^2 cut out by the lines of the plane. It has no g_2^1 and therefore is non hyperelliptic. Futhermore, it possesess g_3^1 without fixed points, of the form K-A, with $A \in \mathscr{K}(\mathbb{F}_8)$. Then $\mathscr{K}$ will be called trigonal [9].

Fig. 1 review all the elements of $\mathscr{K}(\mathbb{F}_8)$.

Any curve considered in the sequel will be defined over $\mathbb{F}_8$. For such a curve $\mathscr{C}$, we denote by $\mathscr{K}\cdot\mathscr{C}$ the associated intersection divisor, rational over $\mathbb{F}_8$.

$$\begin{array}{cccccccc}
P_1 & P_2 & P_3 & P_4 & P_5 & P_6 & P_7 & P_8 \\
\begin{pmatrix}0\\0\\1\end{pmatrix} & \begin{pmatrix}1\\\alpha\\1\end{pmatrix} & \begin{pmatrix}1\\\alpha^2\\1\end{pmatrix} & \begin{pmatrix}1\\\alpha^4\\1\end{pmatrix} & \begin{pmatrix}\alpha\\1\\1\end{pmatrix} & \begin{pmatrix}\alpha\\\alpha^2\\1\end{pmatrix} & \begin{pmatrix}\alpha\\\alpha^6\\1\end{pmatrix} & \begin{pmatrix}\alpha^3\\\alpha^3\\1\end{pmatrix} \\
P_9 & P_{10} & P_{11} & P_{12} & P_{13} & P_{14} & P_{15} & P_{16} \\
\begin{pmatrix}\alpha^3\\\alpha^2\\1\end{pmatrix} & \begin{pmatrix}\alpha^3\\\alpha^5\\1\end{pmatrix} & \begin{pmatrix}\alpha^2\\1\\1\end{pmatrix} & \begin{pmatrix}\alpha^2\\\alpha^4\\1\end{pmatrix} & \begin{pmatrix}\alpha^2\\\alpha^5\\1\end{pmatrix} & \begin{pmatrix}\alpha^6\\\alpha^3\\1\end{pmatrix} & \begin{pmatrix}\alpha^6\\\alpha^6\\1\end{pmatrix} & \begin{pmatrix}\alpha^6\\\alpha^4\\1\end{pmatrix} \\
P_{17} & P_{18} & P_{19} & P_{20} & P_{21} & P_{22} & P_{23} & P_{24} \\
\begin{pmatrix}\alpha^4\\1\\1\end{pmatrix} & \begin{pmatrix}\alpha^4\\\alpha\\1\end{pmatrix} & \begin{pmatrix}\alpha^4\\\alpha^3\\1\end{pmatrix} & \begin{pmatrix}\alpha^5\\\alpha\\1\end{pmatrix} & \begin{pmatrix}\alpha^5\\\alpha^6\\1\end{pmatrix} & \begin{pmatrix}\alpha^5\\\alpha^5\\1\end{pmatrix} & \begin{pmatrix}1\\0\\0\end{pmatrix} & \begin{pmatrix}0\\1\\0\end{pmatrix}
\end{array}$$

Fig. 1. The points of $\mathscr{K}(\mathbb{F}_8)$.

Lemma 4.1. *The nine lines of the projective plane passing through P_1 will be denoted by:*

$$L_i\colon\ Y + \alpha^i X = 0, \quad i \subset \{0,\dots,6\},$$

$$L_7\colon\ X + Z = 0, \qquad L_8\colon\ Y + Z = 0.$$

We have

$$\mathscr{K}\cdot L_i = P_{23} + Q_{a_i} + Q_{b_i} + Q_{c_i}, \quad i \in \{0,\dots,6\},$$

$$\mathscr{K}\cdot L_7 = P_1 + 3P_{23}, \qquad \mathscr{K}\cdot L_8 = 3P_1 + P_{24},$$

where

$$Q_a = \begin{pmatrix} i^2\alpha^3 \\ i^3\alpha^3 \\ 1 \end{pmatrix}, \qquad Q_b = \begin{pmatrix} i^2\alpha^6 \\ i^3\alpha^6 \\ 1 \end{pmatrix}, \qquad Q_c = \begin{pmatrix} i^2\alpha^5 \\ i^3\alpha^5 \\ 1 \end{pmatrix}.$$

Thus these nine lines cover all the 24 elements of $\mathscr{K}(\mathbb{F}_8)$. We shall say that P_1, P_{23}, P_{24} is a flex triangle.

The group of automorphisms of $\mathscr{K}$ is maximal with respect to the Hurwitz bound, with its $168 = 84(g-1)$ elements. Besides, it occurs as a linear projective group defined over $\mathbb{F}_8$ [see 10]. This is why the configuration of Lemma 4.1 described for P_1 carries over to any other point of $\mathscr{K}(\mathbb{F}_8)$. In particular, every point of $\mathscr{K}(\mathbb{F}_8)$ is a flex point and there are eight flex triangles.

We proceed with the two charts shown in Figs. 2 and 3.

We set

$$D_0 = \sum_{i=2}^{22} P_i \quad \text{and} \quad G_0 = 5(P_1 + P_{23} + P_{24})$$

P_1, P_2, P_6, P_{21}	P_1, P_3, P_{10}, P_{12}	P_1, P_4, P_{14}, P_{18}	P_1, P_5, P_9, P_{19}	P_1, P_7, P_{11}, P_{16}
P_1, P_8, P_5, P_{22}	$P_1, P_{13}, P_{17}, P_{20}$	P_2, P_3, P_4, P_{24}	P_2, P_5, P_{13}, P_{16}	P_2, P_7, P_{19}, P_{22}
P_2, P_9, P_{12}, P_{15}	$P_2, P_{10}, P_{14}, P_{17}$	$P_2, P_{18}, P_{20}, P_{23}$	P_3, P_5, P_{14}, P_{21}	P_3, P_6, P_9, P_{23}
P_3, P_7, P_8, P_{13}	$P_3, P_{11}, P_{19}, P_{20}$	$P_3, P_{16}, P_{18}, P_{22}$	P_4, P_6, P_8, P_{20}	P_4, P_7, P_9, P_{17}
$P_4, P_{10}, P_{11}, P_{21}$	$P_4, P_{12}, P_{16}, P_{23}$	$P_4, P_{13}, P_{15}, P_{19}$	P_5, P_6, P_7, P_{24}	P_5, P_8, P_{12}, P_{18}
$P_5, P_{10}, P_{15}, P_{20}$	$P_5, P_{11}, P_{17}, P_{23}$	$P_6, P_{10}, P_{16}, P_{19}$	$P_6, P_{11}, P_{15}, P_{18}$	$P_6, P_{12}, P_{17}, P_{22}$
$P_7, P_{12}, P_{14}, P_{20}$	$P_7, P_{15}, P_{21}, P_{23}$	P_8, P_9, P_{10}, P_{24}	$P_8, P_{14}, P_{19}, P_{23}$	$P_8, P_{16}, P_{17}, P_{21}$
$P_9, P_{11}, P_{14}, P_{22}$	$P_9, P_{13}, P_{18}, P_{21}$	$P_{10}, P_{13}, P_{22}, P_{23}$	$P_{11}, P_{12}, P_{13}, P_{24}$	$P_{14}, P_{15}, P_{16}, P_{24}$
$P_{17}, P_{18}, P_{19}, P_{24}$	$P_{20}, P_{21}, P_{22}, P_{24}$			

Fig. 2. All the 42 collinearity positions between points and $\mathscr{K}(\mathbb{F}_8)$.

P_1, P_{23}, P_{24}	P_2, P_8, P_{11}	P_3, P_{15}, P_{17}	P_4, P_5, P_{22}
P_6, P_{13}, P_{14}	P_7, P_{10}, P_{18}	P_9, P_{16}, P_{20}	P_{12}, P_{19}, P_{21}

Fig. 3. All the eight flex triangles through points of $\mathscr{K}(\mathbb{F}_8)$.

and we define the code

$$G_\Omega(D_0, G_0) = \{(\mathrm{res}_{P_2}(\omega), \ldots, \mathrm{res}_{P_{22}}(\omega)) \in \mathbb{F}_8^{21} \mid \omega \in \Omega(G_0 - D_0)\}$$

with the parameters

$$n = 21, \qquad k = n - \deg G_0 + g - 1 = 8, \qquad d \geq d^* = \deg G_0 + 2 - 2g = 11.$$

Following Pellikaan, in order to decode up to $t^* = \lfloor (d^* - 1)/2 \rfloor = 5$ errors, one has to find an integer s and a s-uple $(F_1, \ldots, F_s)$, where the F_i's are divisors of degree $g + t^* = 8$ such that for every t^*-uple,

$$\mathscr{Q} = (Q_1, \ldots, Q_5); \quad Q_j \in \operatorname{supp} D_0, \ j \in \{1, \ldots, 5\},$$

there exists i, $i \in \{1, \ldots, s\}$, such that the map

$$\varphi(F_i, \mathscr{Q}) : L(G_0 - F_i) \to \mathbb{F}_8^5$$
$$f \mapsto (f(Q_1), \ldots, f(Q_5))$$

is surjective.

This is a key condition for decoding since it provides a practical way of determining a function $\bar{f} \neq 0$ whose set of zeros contains the set of locator of errors.

Moreover, we know that with $s \geq 2$ and $\deg G_0 \geq 4g - 1$, if Ψ^s_{g-1} is not surjective, then such an s-uple does exist [14, Proposition 5]. In our set-up, $s = 3$ turns out to be suitable. So, it means we have to determine three divisors F_1, F_2, F_3 of degree 8 such that for every effective divisors D_1, D_2, D_3 of degree $g - 1 = 2$ the situation

$$F_1 - F_2 \equiv D_1 - D_2, \qquad F_2 - F_3 \equiv D_2 - D_3 \tag{3}$$

cannot arise ($\equiv$ stands for the linear equivalence for the divisors).

Lemma 4.2. *The effective $\mathbb{F}_8$-divisors F on $\mathscr{K}$ of degree* 8 *can be described following the three distinct pattern as*:

(i) $F \equiv 2K$,

(ii) $F \equiv 2K + A - B$; $A, B \in \mathscr{K}(\mathbb{F}_8)$,

(iii) $F \equiv K + \sum_{i=1}^{4} C_i$, $C_i \in \mathscr{K}(\mathbb{F}_8)$, $i \in \{1, \ldots, 4\}$.

Proof. We can always find a cubic curve passing through any set of eight distinct points. Thus, for any divisor F of degree 8. $3K \equiv F + D$ with D divisor of degree 4. Then it yields the three possibilities:

(i) $D \equiv K$, i.e. $F \equiv 2K$.

(ii) $D \in g^1_4$ without fixed point. By [15, Proposition 3.14], every divisor of degree 4, $\mathbb{F}_8$-rational on $\mathscr{K}$ is linearly equivalent to

$$\sum_{i=1}^{4} C_i, \quad C_i \in \mathscr{K}(\mathbb{F}_8), \; i \in \{1, \ldots, 4\}$$

and we can always find a conic curve passing through any set of four points so,

$$2K \equiv D + \sum_{i=1}^{4} C_i \text{ and } F \equiv K + \sum_{i=1}^{4} C_i.$$

(iii) $D \in g^1_3 + B$, $B \in \mathscr{K}(\mathbb{F}_8)$. Thus $D \equiv K - A + B$, $B \in \mathscr{K}(\mathbb{F}_8)$ and $\mathbb{F} \equiv 2K + A - B$. □

The first step is the search of the F_i, $i \in \{1, 2, 3\}$ as listed in (ii), that is, to say

$$F_1 \equiv 2K + A - B, \qquad F_2 \equiv 2K + G - H, \qquad F_3 \equiv 2K + C - E$$

with $A, B, C, E, G, H \in \mathscr{K}(\mathbb{F}_8)$. We see easily that any equality of points in the set $\{A, B, C, E, G, H\}$ results in solutions to system (3). In all generality, the research grows messy due to the non unicity of the conics $\mathscr{C}$ and $\mathscr{C}'$ introduced below. So, at this juncture, we investigate the more tractable situation:

$$F_1 \equiv 2K + A - B, \qquad F_2 \equiv K + \sum_{i=1}^{4} C_i, \qquad F_3 \equiv 2K + C - E,$$

where $A, B, C, E, C_1, C_2, C_3, C_4 \in \mathscr{K}(\mathbb{F}_8)$ are parameters at our disposal to be fixed to suit our purpose. Then we are led to investigate the system:

$$D_1 - D_2 \equiv K + A - \sum_{i=1}^{4} C_i - B, \qquad D_3 - D_2 \equiv K + C - \sum_{i=1}^{4} C_i - E$$

equivalent to

$$B + \sum_{i=1}^{4} C_i \equiv D_2 + \overline{D_1} + A, \qquad E + \sum_{i=1}^{4} C_i \equiv D_2 + \overline{D_3} + C \tag{4}$$

with

$$\overline{D_1} = K - D_1 \quad \text{and} \quad \overline{D_3} = K - D_3.$$

We choose E, B, C_1, C_2, C_3, and C_4 such that no quadruples of $\{E, C_1, C_2, C_3, C_4\}$ and $\{B, C_1, C_2, C_3, C_4\}$ are collinear.

The problem amounts to the following: Let $\mathscr{C}$ be the conic passing through $B + \sum_{i=1}^{4} C_i$ and with residue D_{res}, i.e.

$$\mathscr{K} \cdot \mathscr{C} = B + \sum_{i=1}^{4} C_i + D_{\mathrm{res}}.$$

Accordingly, $\mathscr{C}'$ is the conic such that

$$\mathscr{K} \cdot \mathscr{C} = E + \sum_{i=1}^{4} C_i + D'_{\mathrm{res}}.$$

D_{res} and D'_{res} are divisors of degree 3, $\mathbb{F}_8$-rational. We note $\mathscr{D}_{\mathrm{res}}$ the residues of all the conics passing through D_{res} and A, and $\mathscr{D}'_{\mathrm{res}}$ the residues of all the conics passing through D'_{res} and C. Then, for any divisors D_2, D_1 and D_3 solutions of system (4), we have by the Brill–Noether theorem,

$$D_2 + \overline{D_1} \in \mathscr{D}_{\mathrm{res}}, \tag{5}$$

which yields a set of possible D_2 denoted by $\mathscr{D}$ and

$$D_2 + \overline{D_3} \in \mathscr{D}'_{\mathrm{res}}, \tag{6}$$

which yields another set $\mathscr{D}'$ of possible D_2.

Our final goal is to find

$$A, B, C, E, C_1, C_2, C_3, C_4 \in \mathscr{K}(\mathbb{F}_8)$$

such that

$$\mathscr{D} \cap \mathscr{D}' = \emptyset,$$

or else such that for all divisor D of $\mathscr{D}$, there is no conic passing through D'_{res}, D and C.

Let $\mathscr{D}$ and $D'_{\mathrm{res}} = \alpha' + \beta' + \gamma'$; $\alpha', \beta', \gamma' \in \mathscr{K}(\mathbb{F}_8)$ be given. Then if we assume that

$$K \equiv D_2 + \alpha' + \beta' \tag{7}$$

for every point $C \in \mathscr{K}(\mathbb{F}_8)$, there exists a reducible conic passing through $D_2, \alpha', \beta', \gamma'$, and C, namely the product of the lines (α', β') and (γ', C). So we have $\mathscr{S} \cap \mathscr{S}' \neq \emptyset$. This pattern (7) is consequently to be put aside.

Lemma 4.3. *When*

$$B \notin \{A, E, \alpha', \beta', \gamma'\} \quad \text{and} \quad \alpha', \beta', \gamma' \notin line(A, E),$$

the pattern (7) *cannot arise.*

Proof. If we assume

$$K \equiv D_2 + \alpha' + \beta'$$

then by (6),

$$K \equiv \bar{D}_3 + C + \gamma'.$$

Therefore by (4),

$$\sum_{i=1}^{4} C_i \equiv D_2 + \bar{E} + \bar{\gamma}',$$

where

$$\bar{E} + \bar{\gamma}' \equiv K - (E + \gamma').$$

Returning to (5), we get

$$B + D_1 \equiv A + E + \gamma',$$

which defines a g_3^1. But the restriction set in the lemma have been suitably designed so as to make it impossible. □

We take $B = P_2, \sum_{i=1}^{4} C_i = P_4 + P_9 + P_{19} + P_{20}$ and $A = P_1$. Let $\mathscr{C}$ be the conic:

$$X^2 + \alpha Y^2 + \alpha^3 Z^2 + \alpha^6 XY + \alpha^5 XZ + \alpha^4 YZ = 0.$$

We have

$$\mathscr{C} \cdot \mathscr{K} = B + \sum_{i=1}^{4} C_i + D_{\mathrm{res}}$$

with

$$D_{\mathrm{res}} = \alpha + \beta + \gamma = P_{14} + P_{16} + P_{19}.$$

Let $\mathscr{C}'$ be the conic:

$$X^2 + \alpha^3 Y^2 + \alpha^4 XY + \alpha^2 XZ + \alpha^3 YZ = 0.$$

We have

$$\mathscr{C}' \cdot \mathscr{K} = E + \sum_{i=1}^{4} C_i + D'_{\mathrm{res}}$$

with $E = P_1$ and $D'_{\mathrm{res}} = \alpha' + \beta' + \gamma' = P_5 + P_6 + P_8$. These points satisfy the conditions of Lemma 4.3.

The nine conics $\mathscr{C}_c$, $c \in \{\infty, 0, 1, \ldots, \alpha^6\}$ passing through α, β, γ and A are the conics:

$$\mathscr{C}_c\colon\ X^2 + (\alpha^3 + c\alpha^2)Y^2 + cXY + (\alpha^2 + c\alpha^5)XZ + (\alpha^3 + c\alpha^3)YZ = 0,$$
$$c \in \{0, 1, \ldots, \alpha^6\},$$

and

$$\mathscr{C}_\infty\colon\quad Y^2 + \alpha^5 XY + \alpha XZ + \alpha^3 YZ = 0.$$

We have to calculate $\mathscr{D}$. Listed below are the nine associated intersection divisors:

$$C_0 \cdot \mathscr{K} \equiv 2K \equiv P_1 + P_{14} + P_{16} + P_{19} + \mathscr{P}$$

with $\mathscr{P}$ place of degree 4 over $\mathbb{F}_8$,

$$\mathscr{C}_1 \cdot \mathscr{K} \equiv 2K \equiv P_1 + P_{14} + P_{16} + P_{19} + P_{17} + P_{19} + 2 \cdot P_{22},$$

$$\mathscr{C}_\alpha \cdot \mathscr{K} \equiv 2K \equiv P_1 + P_{14} + P_{16} + P_{19} + P_5 + P_9 + P_{15} + P_{24},$$

$$\mathscr{C}_{a^2} \cdot \mathscr{K} \equiv 2K \equiv P_1 + P_{14} + P_{16} + P_{19} + P_{12} + \mathscr{P}$$

with $\mathscr{P}$ place of degree 3 over $\mathbb{F}_8$,

$$\mathscr{C}_{\alpha^3} \cdot \mathscr{K} \equiv 2K \equiv P_1 + P_{14} + P_{16} + P_{19} + P_2 + 2 \cdot P_3 + P_{16},$$

$$\mathscr{C}_{\alpha^4} \cdot \mathscr{K} \equiv 2K \equiv P_1 + P_{14} + P_{16} + P_{19} + P_1 + P_{14} + P_{20} + P_{21},$$

$$\mathscr{C}_{\alpha^5} \cdot \mathscr{K} \equiv 2K \equiv P_1 + P_{14} + P_{16} + P_{19} + P_{13} + \mathscr{P}$$

with $\mathscr{P}$ place of degree 3 over $\mathbb{F}_8$,

$$\mathscr{C}_{\alpha^6} \cdot \mathscr{K} \equiv 2K \equiv P_1 + P_{14} + P_{16} + P_{19} + P_4 + P_6 + P_{10} + P_{18},$$

$$\mathscr{C}_\infty \cdot \mathscr{K} \equiv 2K \equiv P_1 + P_{14} + P_{16} + P_{19} + P_7 + P_8 + P_{11} + P_{23}.$$

The set $\mathscr{D}$ consists of the 32 divisors shown in Fig. 4.

Now the difficulty lies in finding out a point $\mathscr{C}$ of $\mathscr{K}(\mathbb{F}_8)$ such that for every divisor D of $\mathscr{D}$, the support of the residue with respect to the conics passing through α', β', γ' and D does not contain $\mathscr{C}$.

We have the following collinear 4-tuples:

$$(\alpha', \beta', P_7, P_{24}), \quad (\alpha', \gamma', P_{12}, P_{18}), \qquad (\beta', \gamma', P_4, P_{20}). \tag{8}$$

$P_{17}+P_{19}$	$P_{17}+P_{22}$	$P_{19}+P_{22}$	$2\cdot P_{22}$	P_5+P_9	P_5+P_{15}	P_5+P_{24}	P_9+P_{15}
P_9+P_{24}	$P_{15}+P_{24}$	P_2+P_3	P_2+P_{16}	$2\cdot P_3$	P_3+P_{16}	P_1+P_{14}	P_1+P_{20}
P_1+P_{21}	$P_{14}+P_{20}$	$P_{14}+P_{21}$	$P_{20}+P_{21}$	P_4+P_6	P_4+P_{10}	P_4+P_{18}	P_6+P_{10}
P_6+P_{18}	$P_{10}+P_{18}$	P_7+P_8	P_7+P_{11}	P_7+P_{23}	P_8+P_{11}	P_8+P_{23}	$P_{11}+P_{23}$

Fig. 4. The set of divisors $\mathscr{D}$.

We set $\mathscr{U} = \{P_7, P_{24}, P_{12}, P_{18}, P_4, P_{20}\}$. There are 14 divisors D_2 such that $\operatorname{supp}(D_2) \cap \mathscr{U} \neq \emptyset$ listed as:

$$P_4 + P_6,\quad P_4 + P_{10},\quad P_4 + P_{18},\quad P_7 + P_8,\quad P_7 + P_{11},\quad P_7 + P_{23},\quad P_{18} + P_6,$$

$$P_{18} + P_{10},\ P_{20} + P_1,\ P_{20} + P_{14},\ P_{20} + P_{21},\ P_{24} + P_5,\ P_{24} + P_9,\ P_{24} + P_{15}.$$

For each of them, the conic passing through α', β', γ' and D_2 occurs as reducible, one of the line involved corresponding to one of the collinear 4-tuples of (8).

After some calculation, only the three points P_5, P_{17} and P_{23} among those of $\mathscr{X}(\mathbb{F}_8)$ prove not to be caught in any support of residues with respect to these 14 conics, hence $\mathscr{C} \in \{P_5, P_{17}, P_{23}\}$.

(a) The five divisors D_2:

$$P_2 + P_{16},\quad P_{14} + P_{21},\quad P_{11} + P_{23},\quad P_{17} + P_{22},\quad P_1 + P_{21}$$

are the only one among the 18 remaining divisors of $\mathscr{D}$ such that $\operatorname{supp}(D_2)$ and α' or β' or γ' are collinears. The five related conics are the union of two lines. The former being determined by one of these D_2. The latter by the two remaining points in $\{\alpha', \beta', \gamma'\}$. With respect to these conics, P_{17} belongs to some support of the residues while P_5 and P_{23} are not attained yet so $C \in \{P_5, P_{23}\}$.

(b) The conic

$$X^2 + \alpha^2 Y^2 + \alpha^6 Z^2 + \alpha^3 XY + \alpha^4 XZ + \alpha^2 YZ = 0$$

passes through α', β', γ', $D_2 = P_9 + P_{15}$ and P_5, P_5 is then attained hence $C \in \{P_{23}\}$.

(c) Let us choose $C = P_{23}$. We get the following collinearity positions:

$$(P_{23}, P_{17}, P_{11}, \alpha'),\quad (P_{23}, P_3, P_9, \beta'),\quad (P_{23}, P_{14}, P_{19}, \gamma'). \tag{9}$$

We set $\mathscr{U}_c = (P_{17}, P_{11}, P_3, P_9, P_{14}, P_{19})$. The conics passing through α', β', γ', P_{23} and one of the points of $\mathscr{U}_c$ are the union of two lines: the former determined by one of the collinearity positions of (9) and the latter by the two remaining points in $\{\alpha', \beta', \gamma'\}$. The divisors

$$P_{17} + P_{19},\quad P_{19} + P_{22},\quad P_5 + P_9,\quad P_9 + P_{15},\quad P_2 + P_3,$$

$$2 \cdot P_3,\quad P_3 + P_{16},\quad P_1 + P_{14},\quad P_8 + P_{11}$$

are the nine remaining divisors D_2 among the 13 left such that $\mathrm{supp}(D_2)\cap\mathscr{U}_\infty \neq \emptyset$. However, for each of them, $\sharp\ [\mathrm{supp}(D_2\cap\mathscr{U}_\infty)] = 1 \neq 2$, therefore these divisors do not appear in the intersection with the conics above, which were the only one passing through α', β', γ' and P_{23} liable to catch them. So the remaining possible divisors to solve system (3) are four.

$$P_5 + P_{15}, \qquad P_6 + P_{10}, \quad P_8 + P_{13}, \quad 2 \cdot P_{22}$$

out of the initial set $\mathscr{S}$ with 32 elements.

(d) Up to now, we have confined to exploit extensively rich collinearity configurations among points of $\mathscr{X}(\mathbb{F}_8)$ and we have got all out of it.

To end with the last step let us consider the four conics passing through α', β', γ' and P_{23}:

$$Y^2 + \alpha^4 Z^2 + \alpha^6 XY + XZ + \alpha^2 YZ = 0,$$

$$Y^2 + \alpha^3 Z^2 + XY + \alpha^4 XZ + \alpha^5 YZ = 0,$$

$$Y^2 + \alpha^2 Z^2 + \alpha^3 XY + \alpha^3 YZ = 0,$$

$$Y^2 + \alpha^2 XY + \alpha YZ + \alpha^4 YZ = 0.$$

The support of their residues contains P_{15} but not P_5 (respectively with (P_{10}, P_6), (P_{22}, P_{22}) and (P_8, P_{13})) and so the four remaining divisors are not attained. Consequently, the theorem follows.

Theorem 4.4. *Let F_1, F_2, F_3 be three divisors of degree 8, $\mathbb{F}_8$-rational on $\mathscr{X}$, satisfying*

$$F_1 \equiv 2K + P_1 - P_2, \qquad F_2 \equiv K + P_4 + P_9 + P_{19} + P_{20}, \qquad F_3 \equiv 2K + P_{23} - P_1.$$

Then we have, for any 3-uple $(D_1, D_2, D_3) \in \mathbb{D}_2^3(\mathscr{X})$, the system

$$F_1 - F_2 \equiv D_1 - D_2, \qquad F_2 - F_3 \equiv D_2 - D_3$$

has no solution.

Checking. From now on $C = P_{23}$ is fixed, wae make sure that the orresponding set $\mathscr{S}'$ satisfies $\mathscr{S}\cap\mathscr{S}' = \emptyset$. The nine conics $\mathscr{C}'_c, c \in \{\infty, 0, 1, \ldots, \alpha^6\}$, passing through α', β', γ' and C are the conics

$$\mathscr{C}_c\colon \quad Y^2 + (1 + c\alpha^3)Z^2 + (\alpha^5 + c\alpha^6)XY + (\alpha^5 + c\alpha^2)XZ + cYZ = 0,$$

$$c \in \{0, 1, \ldots, \alpha^6\}$$

and

$$\mathscr{C}_\infty\colon \quad Z^2 + \alpha^3 XY + \alpha^6 XZ + \alpha^4 YZ = 0.$$

Here, below are reviewed the nine intersection divisors:

$$\mathscr{C}_0 \cdot \mathscr{K} \equiv 2K \equiv \alpha' + \beta' + \gamma' + C + P_4 + P_{11} + P_{17} + P_{20},$$

$$\mathscr{C}_1 \cdot \mathscr{K} \equiv 2K \equiv \alpha' + \beta' + \gamma' + C + P_3 + P_9 + P_{12} + P_{18},$$

$$\mathscr{C}_\alpha \cdot \mathscr{K} \equiv 2K \equiv \alpha' + \beta' + \gamma' + C + \mathscr{P}$$

with $\mathscr{P}$ place of degree 4 over $\mathbb{F}_8$,

$$\mathscr{C}_{\alpha^2} \cdot \mathscr{K} \equiv 2K \equiv \alpha' + \beta' + \gamma' + C + P_{15} + P_{16} + \mathscr{P}_1,$$

with $\mathscr{P}_1$ place of degree 2 over $\mathbb{F}_8$,

$$\mathscr{C}_{\alpha^3} \cdot \mathscr{K} \equiv 2K \equiv \alpha' + \beta' + \gamma' + C + P_2 + P_6 + P_{22} + P_{23},$$

$$\mathscr{C}_{\alpha^4} \cdot \mathscr{K} \equiv 2K \equiv \alpha' + \beta' + \gamma' + C + P_1 + P_5 + P_8 + P_{13},$$

$$\mathscr{C}_{\alpha^5} \cdot \mathscr{K} \equiv 2K \equiv \alpha' + \beta' + \gamma' + C + P_{10} + P_{21} + \mathscr{P}_2$$

with $\mathscr{P}$ place of degree 2 over $\mathbb{F}_8$,

$$\mathscr{C}_{\alpha^6} \cdot \mathscr{K} \equiv 2K \equiv \alpha' + \beta' + \gamma' + C + \mathscr{P}$$

with $\mathscr{P}$ place of degree 4 over $\mathbb{F}_8$,

$$\mathscr{C}_{,} \cdot \mathscr{K} \equiv 2K \equiv \alpha' + \beta' + \gamma' + C + P_7 + P_{14} + P_{19} + P_{24}.$$

Then the set $\mathscr{S}'$ of the 33 divisors shown in Fig. 5.

It is then checked $\mathscr{S} \cap \mathscr{S}' = \emptyset$ as primarily announced.

Corollary 4.5. *By means of the divisors of Theorem* 4.4 *Pellikaan algorithm is made effective. We are now in position to decode $C_\Omega(D_0, G_0)$ and so any geometric code $C_\Omega(D, G)$ as well, defined on the Klein quartic over $\mathbb{F}_8$, with odd degree(G) and $d^* \geq 11$, up to $\lfloor (d^* - 1)/2 \rfloor$ errors.*

Corollary 4.6. *For the Klein quartic defined over $\mathbb{F}_8$, the map Ψ^g_{g-1} is not surjective.*

$P_4 + P_{11}$	$P_4 + P_{17}$	$P_4 + P_{20}$	$P_{11} + P_{20}$	$P_{17} + P_{20}$	$P_3 + P_9$	$P_3 + P_{12}$	$P_3 + P_{18}$
$P_9 + P_{12}$	$P_9 + P_{18}$	$P_{12} + P_{18}$	$P_{15} + P_{16}$	$\mathscr{P}_1$	$P_2 + P_6$	$P_2 + P_{22}$	$P_2 + P_{23}$
$P_6 + P_{22}$	$P_6 + P_{23}$	$P_{22} + P_{23}$	$P_1 + P_5$	$P_1 + P_8$	$P_1 + P_{13}$	$P_5 + P_8$	$P_5 + P_{13}$
$P_8 + P_{13}$	$P_{10} + P_{21}$	$\mathscr{P}_2$	$P_7 + P_{14}$	$P_7 + P_{19}$	$P_7 + P_{24}$	$P_{14} + P_{19}$	$P_{14} + P_{24}$
$P_{19} + P_{24}$							

Fig. 5. The set of the divisors $\mathscr{S}'$.

Remark. Through the zeta-function, it can be checked over $\mathbb{F}$, the smallest integer s such that

$$\sharp \mathbb{D}_{(}) < \sharp J_{(})$$

is $g + 1$. It implies that Ψ is not surjective. Corollary 4.6 improves this result, which is as far as we know, the first example treated of this kind.

Acknowledgements

We are very grateful to Jean-Pierre Zanotti and are pleased to express our most sincere thanks for his precious help regarding the implementation of the intersection divisors program, necessary to work out the long and tedious calculations involved in this paper.

References

[1] Ph. Carbonne and A. Thiong Ly, Minimal exponent for Pellikaan's decoding algorithm, in: P. Camion, P. Charpin and S. Harari, eds., Eurocode Udine, 1992, CISM Courses and Lectures, Vol. 339 (Springer, Wien, 1993) 231–253.

[2] I.M. Duursma, Majority coset decoding, IEEE, Trans. Inform. Theory 39 (1993) 1067–1071.

[3] I.M. Duursma, Decoding codes from curves and cyclic codes, Ph.D. Thesis, Eindhoven University of Technology, September 1993.

[4] D. Ehrhard, Über das Dekodieren Algebraisch-Geometrischer Codes, Ph.D. Thesis, University of Düsseldorf, July 1991.

[5] D. Ehrhard, Achieving the designed error capacity in decoding algebraic-geometric codes, IEEE Trans. Inform. Theory 39 (1993) 743–751.

[6] G.L. Feng and T.R.N. Rao, Decoding of algebraic-geometric codes up to the designed minimum distance, IEEE Trans. Inform. Theory 39 (1993) 1–11.

[7] W. Fulton, Algebraic Curves, Math. Lecture Notes Ser. (Benjamin, New York, 1969).

[8] V.D. Goppa, Geometry and Codes, Mathematics and its Applications, Vol. 24 (Kluwer Academic Publishers, Dordrecht, 1991).

[9] J.P. Hansen, Codes on the Klein quartic, ideal and decoding, IEEE Trans. Inform. Theory 33 (6) (1987).

[10] I. Kuribayashi, On certain curves of genus three with many automorphisms, Tsukuba, J. Math. 6(2) (1982) 271–288.

[11] S. Lang, Abelian Varieties, Interscience Tracts in Pure and Applied Mathematics, Vol. 7 (1959).

[12] Matsuaka, On a characterisation of a jacobian variety, Mem. Coll. Sci. Univ. Kyotô 32 (1959) 1–19.

[13] R. Pellikaan, On a decoding algorithm for codes on maximal curves, IEEE Trans. Inform. Theory 35 (1989) 369–381.

[14] D. Rotillon and A. Thiong Ly, Decoding codes on the Klein quartic, in: G.D. Cohen and P. Charpin, eds., Proc. Eurocode 90, Lecture Notes in Computer Science, Vol. 514 (Springer, Berlin, 1991) 135–150.

[15] J.H. van Lint and G. van der Geer, Introduction to Coding Theory and Algebraic Geometry, DMV Seminar 12 (Birkhäuser, Basel, 1988).

[16] S.G. Vlădut, On the decoding of algebraic-geometric codes over $GF(q)$ for $q \geq 16$, IEEE Trans. Inform. Theory 36 (1990) 1461–1463.