Decoding geometric Goppa codes using an extra place

S.C. Porter, B.-Z. Shen and R. Pellikaan *

Appeared in: IEEE Trans. Inform. Theory. IT-**38** (1992), 1663-1676.

Abstract

Decoding geometric Goppa codes can be reduced to solving the key congruence of a received word in an affine ring. If the code length is smaller than the number of rational points on the curve, then this method can correct up to $\frac{1}{2}(d^* - 1) - s$ errors, where d^* is the designed minimum distance of the code and s is the Clifford defect. The affine ring with respect to a place P is the set of all rational functions which have no poles except at P, and it is somehow similar to a polynomial ring. For a special kind of geometric Goppa codes, namely $C_\Omega(D, mP)$, the decoding algorithm is reduced to solving the key equation in the affine ring, which can be carried out by the subresultant sequence in the affine ring with complexity $O(n^3)$, where n is the length of codewords.

Index Terms — Geometric Goppa codes, algebraic-geometric codes, decoding, affine ring, isometry, key equation.

*This work was presented in a talk at IEEE International Symposium on Information Theory 1991, Budapest, Hungary. The first author is with Morrison-Knudsen, Integrated Software Technology Departement, Morrison-Knudsen Plaza IV-7, Boise ID 83707, USA. The last two authors are with the Eindhoven University of Technology, Department of Mathematics and Computing Science, PO Box 513, 5600 MB Eindhoven, The Netherlands.

I Introduction

After Goppa's idea [7],[8],[9],[10] to use algebraic curves over finite fields to construct linear codes and the result of Tsfasman, Vlăduţ and Zink [28], who showed that in this way one can improve the Gilbert-Varshamov bound, it was for some years an open question to find an efficient decoding algorithm for these codes. Justesen, Larsen, Elbrønd Jensen, Havemose and Høholdt [12] found a decoding algorithm for a class of codes on plane curves. This algorithm was generalized by Skorobogatov and Vlăduţ [23] and independently by Krachkovskii [14], to codes on arbitrary curves. We call these codes geometric Goppa codes in this paper, these codes are also called algebraic-geometric. That is if $P_1, \ldots, P_n$ are n rational points on the curve and $D = P_1 + \ldots + P_n$ and G is a divisor with disjoint support with D, then the geometric Goppa code $C_\Omega(D, G)$ is the vector space of all words of the form $(\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega))$, where ω is a differential form in $\Omega(G - D)$. The designed minimum distance of this code is $m - 2g + 2$, where m is the degree of G and g is the genus of the curve, and is denoted by d^*. This decoding algorithm is called the basic algorithm in [23],[29, p.332] and it decodes $\frac{1}{2}\lfloor d^* - 1 - g \rfloor$ errors. The complexity of the basic algorithm is $O(n^3)$, where n is the length of the code, since their method comes down to solving linear equations over a finite field. To correct more errors Skorobogatov and Vlăduţ gave the modified algorithm for a certain class of codes [23], which was extended by Duursma [4] to all geometric Goppa codes. The main idea is to apply the basic algorithm several times untill the correct codeword is obtained. This method can correct up to $\frac{1}{2}(d^* - 1) - s$ errors with complexity $O(n^4)$, where s is the Clifford defect of a set of special divisors [4]. Using the existence of certain divisors Pellikaan [16] showed how the basic algorithm executed in parallel can decode $\frac{1}{2}\lfloor d^* - 1 \rfloor$ errors with complexity $O(n^4)$, if the code comes from a maximal curve. Vlăduţ [30] proved that the restriction to maximal curves is superfluous. It is still a problem to find certain divisors explicitly. In order to decrease the complexity of the algorithm Justesen et al. [13] and Dahl Jensen [11] used Sakata's algorithm, a generalization of the Berlekamp-Massey algorithm to more than one variable.

Around the same time as Justesen et al. [12], Porter found another decoding algorithm, which is a generalization of solving the key equation of classical Goppa codes by Euclid's algorithm in the ring of polynomials in one variable. One can view the ring of polynomials in one variable as the ring of rational functions on the projective line with only poles at the point at infinity. The ring of polynomials in one variable is replaced by the ring $K_\infty(P)$ of rational functions on the curve with only poles at a fixed place P, where P is not equal to one of the rational points used to construct the geometric Goppa code. Euclid's algorithm is replaced by an algorithm using the subresultant sequence, see also Shen [21]. The proofs in the thesis of Porter contain several mistakes and gaps. In this paper we give a correct account of the results of Porter, in more generality and with a greater error correcting capacity. That is to say we can correct up to $\frac{1}{2}(d^* - 1) - s$ errors with complexity $O(n^3)$, if the codelength is smaller than the number of rational points on the curve. Ehrhard [5] also showed that the results of Porter are correct, moreover he gave the connection between the basic algorithm and the decoding by solving the key equation. Shen [22] computed explicit formulas for the syndromes of codes on Hermitian curves and decreased the complexity of solving the key equation for these codes, using the ideas of Sakata.

Outline of the paper

In section II we give the definition of the ring $K_\infty(P)$ and prove that this is an affine ring, using properties of Weierstrass gaps, and prove a division theorem. In section III we show how to get a decoding algorithm of a code from a decoding algorithm for a code isometric to the first one. Furthermore we prove that for every place P not in the support of D, every geometric Goppa code $C_\Omega(D,G)$ is isometric to the code $C_\Omega(D,E-\mu P)$, for some effective divisor E and positive integer μ. In section IV we show that there exist n independent differentials $\varepsilon_1,\ldots,\varepsilon_n \in \Omega(-D-\mu P)$ such that for every differential $\omega \in \Omega(E-\mu P-D)$ we have

$$\omega = \sum \mathrm{res}_{P_i}(\omega)\varepsilon_i.$$

If we let $\varepsilon(\mathbf{x}) = \sum x_i\varepsilon_i$, then

$$\varepsilon(\mathbf{x}) \in \Omega(E-\mu P-D) \text{ if and only if } \mathbf{x} \in C_\Omega(D,E-\mu P).$$

This generalizes the description of classical Goppa codes as follows. Let L be a subset of $\mathbf{F}_q$ and h a Goppa polynomial. Let $L=\{\alpha_1,\ldots\alpha_n\}$. Suppose h is not zero at α_i, for all i. The classical Goppa code $\Gamma(L,h)$ is defined by

$$\Gamma(L,h) = \{\mathbf{x} | \sum \frac{x_i}{X-\alpha_i} \equiv 0 (\mathrm{mod}\ h)\}.$$

If we let $\varepsilon_i = dX/(X-\alpha_i)$, and take for P the point at infinity on the projective line and for E the divisor of zeros of h, then $\Gamma(L,h) = C_\Omega(D,E-P)$ and

$$\mathbf{x} \in \Gamma(L,h) \text{ if and only if } \sum \frac{x_i}{X-\alpha_i}dX \in \Omega(E-P-D)$$

In section V we define the syndrome of a received word. In order to represent the syndrome as a rational function we prove the existence of a particular differential η first. For Goppa polynomial h, the syndrome $S(\mathbf{x})$ of a received word $\mathbf{x}$ is now defined as follows.

$$S(\mathbf{x})\eta = \sum x_i \frac{h(P_i)-h}{h(P_i)}\varepsilon_i.$$

The syndrome is an element of the ring $K_\infty(P)$, and if E is the divisor of zeros of $h \in K_\infty(P)$, then

$$\mathbf{x} \in C_\Omega(D,E-\mu P) \text{ if and only if } S(\mathbf{x}) \equiv 0 (\mathrm{mod}\ h).$$

In section VI we show how to decode $(d^*-1)/2-s$ errors, where s is the Clifford defect, by solving the key equation

$$fS(\mathbf{x}) = r + qh,$$

under a constraint in terms of the degrees of f and r. If the number of errors is at most $(d^*-1)/2-s$ and if (f,r) is a minimal valid solution of the key equation, then $\mathrm{res}_{P_i}(r\eta/f)$ is the error value at place i. In section VII we apply it to codes isometric to $C_\Omega(D,mP)$. Finally in section VIII we give an example showing that in this way one can not in general decode more than the above mentioned number of errors.

Notation

In this paper, $\mathbf{F}$ is a finite field. $\mathcal{X}$ is always a projective, non-singular, absolutely irreducible curve defined over $\mathbf{F}$, and $\mathbf{F}(\mathcal{X})$ is the function field of $\mathcal{X}$ over $\mathbf{F}$. We denote the vector space of rational differential forms on $\mathcal{X}$ over $\mathbf{F}$ by Ω. $P_1, \ldots, P_n$ are n distinct $\mathbf{F}$ -rational points on $\mathcal{X}$, and D is the divisor $P_1 + \cdots + P_n$. Let $G = \sum m_Q Q$ be a divisor on $\mathcal{X}$, then $G_0 = \sum_{m_Q>0} m_Q Q$ and $G_\infty = \sum_{m_Q<0} m_Q Q$. If f is a rational function, then $(f) = \sum v_Q(f)Q$, $(f)_0 = \sum_{v_Q(f)>0} v_Q(f)Q$ and $(f)_\infty = \sum_{v_Q(f)<0} v_Q(f)Q$. Let $\mathcal{O}$ be a finite set of places on $\mathcal{X}$, then we define $(f)_\mathcal{O} = \sum_{Q\in\mathcal{O}} v_Q(f)Q$. Let G_1 and G_2 be divisors on $\mathcal{X}$, if there exists a rational function f such that $G_1 = G_2 + (f)$, then we say that, G_1 and G_2 are linear equivalent and denote it by $G_1 \sim G_2$.

II Affine ring $K_\infty(P)$

Definition 1 Let P be a place of $\mathcal{X}$, define

$$K_\infty(P) = \{f \in \mathbf{F}(\mathcal{X}) | \mathrm{supp}((f)_\infty) \subseteq \{P\}\},$$

we call $K_\infty(P)$ the *affine ring* with respect to P.

Remark 1 . It is easy to see that $K_\infty(P)$ is a subalgebra of the function field $\mathbf{F}(\mathcal{X})$ over $\mathbf{F}$.

Remark 2 . Let $\mathcal{X}$ be embedded in $\mathbf{P}^r$, the projective space of dimension r over $\mathbf{F}$. Let H be a hyperplane in $\mathbf{P}^r$ such that $H \cap \mathcal{X} = \{P\}$. This is always possible by the embedding of $\mathcal{X}$ in the linear system of $(2g+1)P$. As we know there exists a projective change of coordinates T such that $T(H) = \{(x_0 : \ldots : x_r) \in \mathbf{P}^r | x_0 = 0\}$, and $T(H)$ and $T(\mathcal{X})$ intersect in $T(P_\infty)$, so we may assume $H = \{(x_0 : \ldots : x_r) \in \mathbf{P}^r | x_0 = 0\}$ and $H \cap \mathcal{X} = \{P_\infty\}$. Suppose the vanishing ideal $I(\mathcal{X})$ of $\mathcal{X}$ in $\mathbf{P}^r$ is equal to $(F_1, \ldots, F_s)$, where F_i is a homogeneous polynomial in $\mathbf{F}[X_0, \ldots, X_r]$ for every i. Now let $I_* = (F_{1_*}, \ldots, F_{s_*})$ where $F_{i_*}(X_1, \ldots, X_r) = F_i(1, X_1, \ldots, X_r)$, then $\mathcal{X}_* = V(I_*)$ is an affine curve in $\mathbf{A}^r$, the affine space of dimension r over $\mathbf{F}$. For every place Q of $\mathcal{X}$ if Q is not equal to P, then Q_* is a place of $\mathcal{X}_*$, where $Q_* = (x_1/x_0, \ldots, x_r/x_0)$ if $Q = (x_0 : \ldots : x_r)$. Let $\Gamma(\mathcal{X}_*)$ be the affine coordinate ring of $\mathcal{X}_*$, then

$$\mathbf{F}[X_1, \ldots, X_r]/I_* = \Gamma(\mathcal{X}_*) = \bigcap R_Q,$$

where Q runs over all the places of $\mathcal{X}$ except P, and R_Q is the local ring at Q, that is $R_Q = \{f \in \mathbf{F}(\mathcal{X}) | v_Q(f) \geq 0\}$, so

$$\bigcap R_Q = \{f \in \mathbf{F}(\mathcal{X}) | v_Q(f) \geq 0 \text{ for every place } Q \text{ of } \mathcal{X}, Q \neq P\} = K_\infty(P).$$

Therefore $K_\infty(P) = \Gamma(\mathcal{X}_*)$.

Since our decoding algorithm will work on $K_\infty(P)$, it is worth to know some details about this ring. In the following, we will give the construction of $K_\infty(P)$ and a division theorem for $K_\infty(P)$, in the case that P is a place of degree one, that is a rational point.

Definition 2 Let P be a place of $\mathcal{X}$ of degree one, let n be a non-negative integer. If $l(nP) = l((n-1)P)$, then n is called a *(Weierstrass) gap* of P.

Proposition 1 *Let $\mathcal{X}$ be a curve of genus $g \geq 1$ and let P be a place of degree one of $\mathcal{X}$. then*

a) $1 = l(0) \leq l(P) \leq \cdots \leq l((2g-1)P) = g$. *So there are exactly g gaps of P.*

b) *Let $m \in \mathbf{N}$. Then m is a non-gap of P if and only if there exists an $f \in L(mP)$, such that $v_P(f) = -m$.*

c) *If m_1 and m_2 are non-gaps of P, then $m_1 + m_2$ is also a non-gap of P.*

Proof. See [6]

Lemma 1 *If r is a gap of P, then there exists an integer t with $1 \leq t \leq \lfloor (2g+1-r)/2 \rfloor$, such that $2g+1-t$ and $r+t$ are both non-gaps.*

Proof. Let $n_1, \ldots, n_g$ be all gaps of P. For all $s \in \{1, \ldots, \lfloor r/2 \rfloor\}$ either s or $r-s$ is a gap by Proposition 1.c, since r is a gap. Suppose $1 \leq s \leq r/2$ then $r/2 \leq r-s < r$, so if $s_1, s_2 \in \{1, \ldots, \lfloor r/2 \rfloor\}$ and $s_1 \neq s_2$, then $r - s_1 \neq s_2$. Thus

$$\#\{n_i < r | 1 \leq i \leq g\} \geq \lfloor \frac{r}{2} \rfloor.$$

If the assertion of this lemma is not true, then for all $t \in \{1, \ldots, \lfloor (2g+1-r)/2 \rfloor\}$ either $2g+1-t$ or $r+t$ is a gap. Suppose $1 \leq t \leq (2g+1-r)/2$ then $(2g+1+r)/2 \leq 2g+1-t \leq 2g$ and $r+1 \leq r+t \leq (2g+1+r)/2$. So if $t_1, t_2 \in \{1, \ldots, \lfloor (2g+1-r)/2 \rfloor\}$ and $t_1 \neq t_2$, then $2g+1-t_1 \neq r+t_2$. Thus

$$\#\{n_i > r | 1 \leq i \leq g\} \geq \lfloor \frac{2g+1-r}{2} \rfloor.$$

Therefore, by the above and the assumption that r is also a gap, one gets

$$g \geq \lfloor \frac{r}{2} \rfloor + \lfloor \frac{2g+1-r}{2} \rfloor + 1 = g+1,$$

a contradication. □

Proposition 2 *Let $0 = m_0 < m_1 < \cdots < m_{g-1} < m_g = 2g < m_{g+1} = 2g+1$ be all the non-gaps of P between 0 and $2g+1$. If $m \in \mathbf{N}$ is a non-gap of P, then*

$$m = \sum_{i=0}^{g+1} k_i m_i,$$

where $k_i \in \mathbf{N}$ for all i.

Proof. If $0 \leq m \leq 2g+1$ then the result is trivial. Now we consider the case that $m \geq 2g+2$. Let $m = k(2g+1) + r$, where $0 \leq r \leq 2g$ and $k \geq 1$, then

i) if r is a non-gap, then there is an i such that $r = m_i$. Thus $m = m_i + k m_{g+1}$.

ii) if r is a gap, then by Lemma 1 there exists a $t \in \mathbf{N}$ with $1 \leq t \leq \lfloor (2g+1-r)/2 \rfloor$, such that $2g-t+1$ and $r+t$ are non-gaps of P. So there exist i, j with $1 \leq i, j \leq g+1$ such that $r+t = m_i$ and $2g+1-t = m_j$. Thus $2g+1+r = r+t+2g+1-t = m_i + m_j$. Therefore $m = (k-1)(2g+1) + (2g+1+r) = (k-1)m_{g+1} + m_i + m_j$. □

Proposition 3 *Let $0 = m_0 < m_1 < \cdots < m_{g-1} < m_g = 2g < m_{g+1} = 2g+1$ be all the non-gaps of P between 0 and $2g+1$. Let $f_i \in L(m_iP)$ with $v_P(f_i) = -m_i$. Then for every $m \in \mathbf{N}$, the vector space $L(mP)$ is generated by*

$$\left\{ \prod_{i=0}^{g+1} f_i^{k_i} | \sum_{i=0}^{g+1} k_i m_i \leq m, \text{ with } \quad k_i \in \mathbf{N} \text{ for all } i \right\},$$

Proof. If m is a gap of P, then there exists an m_i such that $L(mP) = L(m_iP)$ by the definition of a gap. So we may assume that m is a non-gap of P.

We first order all the non-gaps as follows $0 = m_0 < m_1 < m_2 < \cdots < m_{g-1} < m_g = 2g < m_{g+1} = 2g+1 < \cdots < m_{g+l} = 2g+l < \cdots$. For every $k \in \mathbf{N}$, let the vector space generated by

$$\left\{ \prod_{i=0}^{g+1} f_i^{k_i} | \sum_{i=0}^{g+1} k_i m_i \leq m_k, \text{ with } \quad k_i \in \mathbf{N} \text{ for all } i \right\},$$

be denoted by L_k, in particular $L_k \subseteq L(m_kP)$.

Now we prove the proposition by induction on k.

1) If $k = 0$, then $m_0 = 0$, so $L(m_0P) = L(0) = \mathbf{F} = L_0$.

2) Suppose $L(m_kP) = L_k$. Then

$$L(m_{k+1}P) \supseteq L_{k+1} \supseteq L_k = L(m_kP),$$

by the induction hypothesis. Now we consider the dimension of L_{k+1}. Since m_{k+1} is a non-gap, there esist non negative integers $k_0, \ldots, k_{g+1}$ such that $m_{k+1} = \sum_{i=0}^{g+1} k_i m_i$, by Proposition 2. Put $f = \prod_{i=0}^{g+1} f_i^{k_i}$, then $v_P(f) = -m_{k+1}$. Thus $f \in L_{k+1}$ but $f \notin L(m_kP)$, therefore

$$l(m_{k+1}P) \geq \dim(L_{k+1}) \geq l(m_kP) + 1.$$

But $l(m_{k+1}P) \leq l(m_kP) + 1$ by the definition of the sequence $\{m_k\}_{i=0}^{\infty}$. So $l(m_{k+1}P) = \dim(L_{k+1})$. Thus finally $L(m_{k+1}P) = L_{k+1}$. □

Theorem 1 *Let $m_0 < \cdots < m_{g+1}$ be all the non-gaps of P between 0 and $2g+1$, let $f_i \in L(m_iP)$ such that $v_P(f_i) = -m_i$ for $i = 0, \ldots, g+1$. Then*

$$K_\infty(P) = \mathbf{F}[f_1, f_2, \ldots, f_{g+1}].$$

So that

$$K_\infty(P) \cong \mathbf{F}[X_1, \ldots, X_{g+1}]/I,$$

where I is some ideal of the polynomial ring $\mathbf{F}[X_1, \ldots, X_{g+1}]$.

Proof. One has $K_\infty(P) = \bigcup_{m=0}^{\infty} L(mP)$, which is generated by the elements $\prod_{i=0}^{g+1} f_i^{k_i}$, by Proposition 3 and $f_0 \in \mathbf{F}$. Thus $K_\infty(P) \subseteq \mathbf{F}[f_1, f_2, \ldots, f_{g+1}]$. On the other hand, $\mathbf{F}[f_1, \ldots, f_{g+1}] \subseteq K_\infty(P)$ since $f_i \in K_\infty(P)$ for all $i = 1, \ldots, g+1$ and $K_\infty(P)$ is a ring. Therefore

$$K_\infty(P) = \mathbf{F}[f_1, f_2, \ldots, f_{g+1}].$$

□

Example 1 The projective line $\mathbf{P}^1$ over $\mathbf{F}$. If $P = (1:0)$ and $1/x$ is a local parameter at P, then $K_\infty(P) = \mathbf{F}[x]$.

Example 2 *The Hermitian curve $H(q)$ is defined by the equation*

$$U^{q+1} + V^{q+1} + W^{q+1} = 0$$

over $GF(q^2)$ (for the details we refer to [24, 27]). Let $a, b \in GF(q^2)$ such that $a^q + a = b^{q+1} = -1$ and $P = (1 : b : 0)$. The set of non-gaps of P is $\{iq + j(q+1) | i, j \in \mathbf{N}\}$. Let $u = U/W$ and $v = V/W$. Define $x = b/(v - bu)$ and $y = ux - a$. Hence we have $K_\infty(P) = \mathbf{F}[x, y]$, where $x^{q+1} = y^q + y$.

Example 3 *The curve $\mathcal{X}(l, q)$ in $\mathbf{P}^l$ is defined by the equations*

$$X_i^{q+1} - X_i^2 X_0^{q-1} + X_{i+1} X_0^q - X_{i+1}^q X_0 = 0 \text{ for } i = 1, \ldots, l-1$$

over $GF(q^2)$ (see [17]). From [17] we know that $L(m\tilde{P}_\infty)$ is generated by the set

$$\{z_1^{k_1} \cdots z_l^{k_l} | \sum_{i=1}^{l} k_i q^{l-i} (q+1)^{i-1} \leq m\},$$

where $z_i = y_i \circ n$, and n is the normalization of $\mathcal{X}(l, q)$ and $\tilde{P}_\infty$ is the unique rational point of $n^{-1}(P_\infty)$, and $y_i = X_i/X_0$. Hence $K_\infty(P_\infty) = \mathbf{F}[z_1, \ldots, z_l]$.

Definition 3 Define the map

$$\deg : K_\infty(P) \longrightarrow \mathbf{N} \cup \{-\infty\}$$

by $\deg(f) = -v_P(f)$ and $\deg(f) = -\infty$ if and only if $f = 0$.

Remark 3 Notice that we now have an abuse of notation, deg is a map on the set of divisors and on $K_\infty(P)$. If f is a rational function, then

$$\deg((f)) = 0 \text{ and } \deg((f)_0) = \deg((f)_\infty).$$

Hence for every $f \in K_\infty(P)$, $\deg(f) = \deg((f)_\infty) = \deg((f)_0)$.

Remark 4 If P is a rational point, then

$$\mathbf{N} \setminus \text{Image}(\deg) = \{n_1, \ldots, n_g\},$$

is the set of gaps of P.

Lemma 2 *If $f, h \in K_\infty(P)$ then*
i) $\deg(fh) = \deg(f) + \deg(h)$*;*
ii) $\deg(f + h) \leq \max\{\deg(f), \deg(h)\}$*, furthermore* $\deg(f + h) = \deg(f)$ *if* $\deg(f) > \deg(h)$.

Proof. This follows immediately from the corresponding properties of the discrete valuation v_P. □

Remark 5 . If P is a rational point and the genus is not zero, then $K_\infty(P)$ with the map deg is not an Euclidean domain. In fact, given an $f \in K_\infty(P)$ with $\deg(f) > 0$, there exists a gap n such that $\deg(f) + n$ is not a gap. So there exists an $f' \in K_\infty(P)$ such that $\deg(f') = \deg(f)+n$. Suppose $K_\infty(P)$ is an Euclidean domain, then there exist $q, r \in K_\infty(P)$ such that $f' = qf + r$ with $0 \leq \deg(r) < \deg(f)$. Hence $q \neq 0$ and $\deg(f') = \deg(q) + \deg(f)$. Thus $n = \deg(q)$ is not a gap, which is a contradiction.

Although $K_\infty(P)$ with the map deg is not an Euclidean domain in case P is a rational point and the genus is not zero, we still can prove a division theorem. We need a lemma and a definition first.

Lemma 3 *Let P be a rational point. Suppose $f, h \in K_\infty(P)$, and $n = \deg(f) = \deg(h)$, then there exists a unique $\alpha \in \mathbf{F}$, such that $\deg(f - \alpha h) < n$.*

Proof. The vector space $L(nP)/L((n-1)P)$ is at most one dimensional. f and h are elements of $L(nP)$ and not of $L((n-1)P)$, since $\deg(f) = \deg(h) = n$. Hence $f + L((n-1)P), h + L((n-1)P)$ are linearly dependent and not equal to $L((n-1)P)$. Thus there exists a unique $\alpha \in \mathbf{F}$ such that $f - \alpha h \in L((n-1)P)$. Therefore $\deg(f - \alpha h) < n$. □

Definition 4 . Let P be a rational point. Let $m \in \mathbf{N}$. Define

$$gap(m) = \{0, 1, \ldots, m-1, m+n_1, \ldots, m+n_g\},$$

where $n_1, \ldots, n_g$ are the gaps of P. For a nonzero element h of $K_\infty(P)$ we define

$$\mathrm{gap}(h) = \mathrm{gap}(\deg(h)).$$

Theorem 2 (Division Theorem). *Let P be a rational point. For every $f, h \in K_\infty(P)$, $h \neq 0$, there exist $q, r \in K_\infty(P)$, such that $f = qh + r$ and $r = 0$ or $\deg(r) \in gap(h)$. Moreover, $\deg(r)$ is unique, that is, if there are another $q', r' \in K_\infty(P)$ such that $f = q'h + r'$, and $r' = 0$ or $\deg(r') \in gap(h)$, then $\deg(r') = \deg(r)$ or $r = r' = 0$.*

Proof. We prove the existence by induction on $\deg(f)$.

1) If $f = 0$ then take $q = r = 0$.

2) If $\deg(f) \in \mathrm{gap}(h)$, then take $q = 0$ and $r = f$.

3) If $\deg(f) \notin \mathrm{gap}(h)$, then $\deg(f) \geq \deg(h)$ and $\deg(f) - \deg(h)$ is not a gap. Hence there exists a $q_0 \in K_\infty(P)$ such that $\deg(q_0) = \deg(f) - \deg(h)$, so $\deg(f) = \deg(q_0 h)$. Hence $\deg(f - \alpha q_0 h) < \deg(f)$ for some $\alpha \in \mathbf{F}$, by Lemma 3. By the induction hypothesis there exist $q_1, r \in K_\infty$ such that $f - \alpha q_0 h = q_1 h + r$, and $\deg(r) \in \mathrm{gap}(h)$. Therefore $f = qh + r$ where $q = q_1 + \alpha q_0$ and $\deg(r) \in \mathrm{gap}(h)$, or $r = 0$.

Now we prove the uniqueness. If there are another $q', r' \in K_\infty(P)$ such that $f = q'h + r'$ with $r' = 0$ or $\deg(r') \in \mathrm{gap}(h)$, then $(q - q')h = r' - r$. If $r = 0$ and $r' \neq 0$ then $\deg(r') = \deg(h) + \deg(q - q')$ which is not an element of $\mathrm{gap}(h)$, since $\deg(q - q')$ is not a gap, a contradiction. Thus $r = 0$ if and only if $r' = 0$. If both r and r' are nonzero and $\deg(r') \neq \deg(r)$, say $\deg(r) > \deg(r')$, then $\deg(r) = \deg(q - q') + \deg(h) \notin \mathrm{gap}(h)$ since $\deg(q - q')$ is not a gap, a contradiction. Thus $\deg(r) = \deg(r')$. □

III Geometric Goppa codes and isometry

Let Ω be the vector space of rational differential forms on $\mathcal{X}$ over $\mathbf{F}$.

Definition 5 . Define the map

$$\alpha_\Omega : \Omega \longrightarrow \mathbf{F}^n$$

by

$$\omega \mapsto (\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega)).$$

Definition 6 Let G be a divisor on $\mathcal{X}$ such that $\mathrm{supp}(G) \cap \mathrm{supp}(D) = \emptyset$, then the geometric Goppa code $C_\Omega(D, G)$ is defined by $\mathrm{Image}(\alpha_\Omega|_{\Omega(G-D)})$.

Theorem 3 *(Goppa). If $m = \deg(G) \geq 2g - 1$, then the restriction of α_Ω to $\Omega(G - D)$ is injective, and $C_\Omega(D, G)$ is a linear $[n, k, d]$ code with*

$$k \geq n - m - 1 + g, \quad \textit{and} \quad d \geq m - 2g + 2,$$

If moreover $m < n$, then $k = n - m - 1 + g$. We call $m - 2g + 2$ the designed minimum distance of $C_\Omega(D, G)$ and denote it by d^*. Furthermore, if $\omega_1, \ldots, \omega_k$ is a basis of $\Omega(G - D)$, and

$$A = \begin{pmatrix} \mathrm{res}_{P_1}(\omega_1) & \ldots & \mathrm{res}_{P_n}(\omega_1) \\ \vdots & \ddots & \vdots \\ \mathrm{res}_{P_1}(\omega_k) & \ldots & \mathrm{res}_{P_n}(\omega_k) \end{pmatrix},$$

then A has rank k and is a generator matrix of $C_\Omega(D, G)$.

Proof. See [7, 8, 9, 10, 15] and [29].

Definition 7 Let C be a linear code in $\mathbf{F}^n$ and σ a permutation of $\{1, \ldots, n\}$. Define $\sigma\mathbf{x} = (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ and $\sigma C = \{\sigma\mathbf{x} | \mathbf{x} \in C\}$. Two linear codes C_1 and C_2 in $\mathbf{F}^n$ are called *equivalent* if $C_2 = \sigma C_1$ for some permutation σ of $\{1, \ldots, n\}$. Let $\lambda = (\lambda_1, \ldots, \lambda_n)$ be an n-tuple of non zero elements in $\mathbf{F}$. Define $\lambda\mathbf{x} = (\lambda_1 x_1, \ldots, \lambda_n x_n)$ and $\lambda C = \{\lambda\mathbf{x} | \mathbf{x} \in C\}$. The codes C_1 and C_2 are called *generalized equivalent* or *isometric* if there is an n-tuple $\lambda = (\lambda_1, \ldots, \lambda_n)$ of nonzero elements in $\mathbf{F}$ and a permutation σ such that $C_2 = \lambda\sigma C_1$. We call λ the scaling factor.

Remark 6 We can view $\lambda\sigma$ as a linear map of $\mathbf{F}^n$ which leaves the Hamming metric invariant. Note that a linear map of $\mathbf{F}^n$ leaves the Hamming metric invariant if and only if it is of the form $\lambda\sigma$.

Definition 8 Let C_1 and C_2 be two isometric codes in $\mathbf{F}^n$, that is $C_2 = \lambda\sigma C_1$ for some permutation σ and scaling factor λ. Suppose $A(C_1)$ is a decoding algorithm of C_1, the induced decoding algorithm $\lambda\sigma A(C_1)$ is defined as follows,
(1) input $\boldsymbol{x}$;
(2) $\boldsymbol{y} := \sigma^{-1}(x_1/\lambda_1, \ldots, x_n/\lambda_n)$;
(3) run $A(C_1)$ with input $\boldsymbol{y}$ to get $\boldsymbol{c}' \in C_1$;
(4) output $\boldsymbol{c} := \lambda\sigma\boldsymbol{c}'$;
(5) stop.

The following proposition follows immediately from the above definition.

Proposition 4 *Let C_1 and C_2 be isometric codes in $\mathbf{F}^n$, that is $C_2 = \lambda\sigma C_1$ for some permutaion σ and scaling factor λ. Suppose the algorithm $A(C_1)$ decodes C_1 upto e errors. Then the induced algorithm $\lambda\sigma A(C_1)$ decodes C_2 upto e errors too.*

Remark 7 By the above definition and Proposition 4, we see that, as soon as a decoding algorithm of one of the codes in an isometry class is given, all the decoding algorithms of the codes in this class are given by the induced algorithms and they correct the same number of errors. In the rest of this section, we will give a special class leader of every isometry class for which a decoding algorithm will be given later. First, the following proposition gives a sufficient condition for two geometric Goppa codes to be isometric.

Proposition 5 *Let G_1 and G_2 be two linear equivalent divisors such that G_i and D have disjoint support, where $i = 1, 2$. Suppose there is a rational function f with disjoint support with D, such that $G_1 = G_2 + (f)$. Then*

$$C_\Omega(D, G_2) = \lambda C_\Omega(D, G_1),$$

where $\lambda = (f(P_1), \ldots, f(P_n))$.

Proof. See [26]. □

Proposition 6 *Let H be an effective divisor such that $\mathcal{H} \cap \{P_1, \ldots, P_n\} = \emptyset$, where $\mathcal{H} = \mathrm{supp}(H)$. Let P be a place of $\mathcal{X}$ which is not in $\mathcal{H} \cup \{P_1, \ldots, P_n\}$. Then there exists an $h \in K_\infty(P)$, such that $(h)_\mathcal{H} = H$ and $\mathrm{supp}((h)) \cap \{P_1, \ldots, P_n\} = \emptyset$.*

Proof. Suppose $H = \sum_{i=1}^m b_i' Q_i$, where $b_i' \geq 0$ for $i = 1, \ldots, m$, so $\mathcal{H} = \{Q_1, \ldots, Q_m\}$. Define $Q_{m+i} = P_i$ for $i = 1, \ldots, n$, and define $b_i = b_i' + 1$ if $i = 1, \ldots, m$ and $b_i = 1$ if $i = m+1, \ldots, m+n$. Now choose an integer k, such that

$$k \deg(P) - \sum_{i=1}^{m+n} b_i \deg(Q_i) \geq 2g - 1.$$

So

$$k \deg(P) - \sum_{i=1}^{m+n} b_i \deg(Q_i) + \deg(Q_j) > 2g - 1,$$

for every j. Hence

$$l(kP - \sum_{i=1}^{m+n} b_i Q_i + Q_j) = l(kP - \sum_{i=1}^{m+n} b_i Q_i) + \deg Q_j,$$

for every j, by the Riemann-Roch Theorem. Therefore $L(kP - \sum_{i=1}^{m+n} b_i Q_i + Q_j)$ contains $L(kP - \sum_{i=1}^{m+n} b_i Q_i)$ as a proper subspace. Thus for every j there exists an h_j in the first mentioned space and not in the last one. So $h_j \in K_\infty(P)$, and $v_{Q_j}(h_j) = b_j - 1$ and $v_{Q_i}(h_j) \geq b_i$ if $i \neq j$. Now define $h = \sum_{j=1}^{m+n} h_j$, then $h \in K_\infty(P)$ and

$$(h)_{\mathcal{H}'} = \sum_{i=1}^{m+n} (b_i - 1) Q_i = \sum_{i=1}^{m} b_i' Q_i = H \text{ ,where } \mathcal{H}' = \{Q_1, \ldots, Q_{m+n}\}.$$

Hence $(h)_{\mathcal{H}} = H$ and $v_{P_i}(h) = v_{Q_{m+i}}(h) = 0$ for $i = 1, \ldots, n$, that is

$$\operatorname{supp}((h)) \cap \{P_1, \ldots, P_n\} = \emptyset.$$

□

Lemma 4 *Let G be a nonzero divisor such that G and D have disjoint support. Let P be a place not in $\{P_1, \ldots, P_n\}$. Then there exists a rational function f, such that G' and $D + P$ have disjoint support, $G' = G + (f)$ is a non-effective divisor and $v_{P_i}(f) = 0$ for $i \in \{1, \ldots, n\}$*

Proof. Suppose $v_P(G) = v$. Choose a place Q, such that $Q \notin \{P_1, \ldots, P_n, P\} \cup \operatorname{supp}(G)$. There exists a rational function f such that $v_Q(f) = -1$, $v_P(f) = -v$ and $v_{P_i}(f) = 0$ for all $i = 1, \ldots, n$, by the independence of valuations, see [1, p. 11]. Hence $G' := G + (f)$ is a non-effective divisor since $v_Q(G + (f)) = v_Q(f) = -1$ and $\operatorname{supp}(G') \cap \{P_1, \ldots, P_n, P\} = \emptyset$. □

Proposition 7 *Let P be an extra place, that is a place not in $\{P_1, \ldots, P_n\}$. Let G be a divisor such that G and D have disjoint support. Then there exist an effective divisor E and a positive integer μ, such that $C_\Omega(D, G)$ and $C_\Omega(D, E - \mu P)$ are isometric.*

Proof. First there exists a rational function f such that if we define $G' = G + (f)$, then $G'_\infty \neq 0$, $\operatorname{supp}(G') \cap \{P_1, \ldots, P_n, P\} = \emptyset$ and $v_{P_i}(f) = 0$ for $i \in \{1, \ldots, n\}$ by Lemma 4. Hence $f(P_i)$ exists and is not equal to zero for every $i \in \{1, \ldots, n\}$. Now by Proposition 6, there exists an $h \in K_\infty(P)$ such that $(h)_{\mathcal{H}} = G'_\infty$, where $\mathcal{H} = \operatorname{supp}(G'_\infty)$ and $\operatorname{supp}((h)) \cap \{P_1, \ldots, P_n\} = \emptyset$. Thus $h(P_i)$ exists and $h(P_i) \neq 0$ for all $i = 1, \ldots, n$. Now define $E = G' + (h)_0$, then $E \geq G'_0 - G'_\infty + (h)_{\mathcal{H}} \geq 0$, this means that E is an effective divisor. Moreover E and D have disjoint support, since $\operatorname{supp}(E) \subseteq \operatorname{supp}(G') \cup \operatorname{supp}((h)_0)$ and G' and $(h)_0$ have disjoint support with D. Take $\mu = -v_P(h)$, then $\mu \geq \deg(G'_\infty) > 0$ and

$$E - \mu P = G' + (h)_0 - (h)_\infty = G + (fh),$$

since $h \in K_\infty(P)$. Therefore $C_\Omega(D, G) \simeq C_\Omega(D, E - \mu P)$ by Proposition 5. This proves our proposition. □

Proposition 8 *Let P be an extra place. Let m be an integer. Then there exists an $h \in K_\infty(P)$ and a positive integer μ, such that $C_\Omega(D, mP)$ and $C_\Omega(D, (h)_0 - \mu P)$ are isometric.*

Proof. By Proposition 6, there exists an $h \in K_\infty(P)$ such that (h) and D have disjoint support and $\deg(h) > m$. Let $\mu = \deg(h) - m$, then μ is a positive integer and

$$(h)_0 - \mu P = (h) + mP.$$

Therefore $C_\Omega(D, (h)_0 - \mu P)$ and $C_\Omega(D, mP)$ are isometric by Proposition 5. □

IV The residue representation of differentials

Before we define the syndrome of the code $C_\Omega(D, E - \mu P)$, in this section we will give the representation of every differential $\omega \in \Omega(E - \mu P - D)$ by its residues at the points $P_1, \ldots, P_n$.

Proposition 9 *Let P be a place not in $\{P_1, \ldots, P_n\}$ and let μ be a positive integer. Then*

$$\Omega(-D-\mu P)/\Omega(-\mu P) \cong \mathbf{F}^n \ .$$

Proof. The restriction of α_Ω to $\Omega(-D-\mu P)$ is an homomorphism from $\Omega(-D-\mu P)$ to $\mathbf{F}^n$ with kernel $\Omega(-\mu P)$. Furthermore, by the Riemann-Roch Theorem we have that the difference between the dimensions of $\Omega(-D-\mu P)$ and $\Omega(-\mu P)$ is n. □

Proposition 10 *Let P be a place not in $\{P_1, \ldots, P_n\}$ and let μ be a positive integer. Then for every $i \in \{1, \ldots, n\}$ there exists an $\varepsilon_i \in \Omega(-P_i - \mu P)$ such that $\mathrm{res}_{P_i}(\varepsilon_i) = 1$. Therefore $\{\overline{\varepsilon_i} := \varepsilon_i + \Omega(-\mu P)\}_{i=1}^n$ is a basis of $\Omega(-D-\mu P)/\Omega(-\mu P)$, and for every $\omega \in \Omega(-D-\mu P)$,*

$$\overline{\omega} := \omega + \Omega(-\mu P) = \sum_{i=1}^{n} \mathrm{res}_{P_i}(\omega)\overline{\varepsilon}_i.$$

Proof. By Proposition 9, we have

$$\Omega(-P_i - \mu P)/\Omega(-\mu P) \cong \mathbf{F},$$

where $i = 1, \ldots, n$. Hence there exists an $\omega_i \in \Omega(-P_i - \mu P)$ such that $\omega_i \notin \Omega(-\mu P)$, so $v_{P_i}(\omega_i) = -1$. Now define the differential $\varepsilon_i = \omega_i / \mathrm{res}_P(\omega_i)$, then $\varepsilon_i \in \Omega(-P_i - \mu P)$ and $\mathrm{res}_{P_i}(\varepsilon_i) = 1$.

Now suppose there exist $a_1, a_2, \ldots, a_n \in \mathbf{F}$ such that $\sum_{i=1}^n a_i \overline{\varepsilon_i} = \overline{0}$, that is $\sum_{i=1}^n a_i \varepsilon_i \in \Omega(-\mu P)$. We claim that all a_i are zero. Otherwise there exists a $j \in \{1, \ldots, n\}$, such that $a_j \neq 0$. So $v_{P_j}(\sum_{i=1}^n a_i \varepsilon_i) = -1$, hence $\sum_{i=1}^n a_i \varepsilon_i \notin \Omega(-\mu P)$, a contradication. Thus $\overline{\varepsilon_1}, \ldots, \overline{\varepsilon_n}$ are linearly independent. Hence it is a basis of $\Omega(-D-\mu P)/\Omega(-\mu P)$, since this last mentioned space has dimension n, by Proposition 9. Therefore, for every $\omega \in \Omega(-D-\mu P)$, there exist $a_1, \ldots, a_n \in \mathbf{F}$ such that

$$\overline{\omega} = \sum_{i=1}^{n} a_i \overline{\varepsilon_i}.$$

This means that there exists an $\omega' \in \Omega(-\mu P)$, such that

$$\omega = \sum_{i=1}^{n} a_i \varepsilon_i + \omega'.$$

After calculating the residue of P_i on both sides, we get

$$\mathrm{res}_{P_i}(\omega) = a_i.$$

Thus

$$\overline{\omega} = \sum_{i=1}^{n} \mathrm{res}_{P_i}(\omega)\overline{\varepsilon_i}.$$

□

Proposition 11 *Let P be a place not in $\{P_1, \ldots, P_n\}$. Let E be an effective divisor and let μ be a positive integer, such that E and D have disjoint support and $\deg(E - \mu P) \geq 2g - 1$. Then there exist n differentials $\varepsilon_1, \ldots, \varepsilon_n$, which are independent modulo $\Omega(-\mu P)$, such that $\varepsilon_i \in \Omega(-P_i - \mu P)$ and $\mathrm{res}_{P_i}(\varepsilon_i) = 1$, and for every $\omega \in \Omega(E - \mu P - D)$*

$$\omega = \sum_{i=1}^{n} \mathrm{res}_{P_i}(\omega)\varepsilon_i.$$

If moreover $\mu = 1$, then $(\varepsilon_i)_\infty = P_i + P$ for all i.

Proof. By Proposition 10, there exist $\eta_1, \ldots, \eta_n \in \Omega(-D-\mu P)$, such that $\eta_i \in \Omega(-P_i-\mu P)$ and $\mathrm{res}_{P_i}(\eta_i) = 1$ for $i = 1, \ldots, n$, and $\overline{\eta_1}, \ldots, \overline{\eta_n}$ is a basis of $\Omega(-D-\mu P)/\Omega(-\mu P)$. Now let $\omega_1, \omega_2, \ldots, \omega_k$ be a basis of $\Omega(E-\mu P-D)$, which is a subset of $\Omega(-\mu P-D)$. Thus

$$\overline{\omega_i} = \sum_{j=1}^{n} \mathrm{res}_{P_j}(\omega_i)\overline{\eta_j} \quad \text{for } i = 1, \ldots, k,$$

by Proposition 10. Define

$$A = \begin{pmatrix} \mathrm{res}_{P_1}(\omega_1) & \ldots & \mathrm{res}_{P_n}(\omega_1) \\ \vdots & \ddots & \vdots \\ \mathrm{res}_{P_1}(\omega_k) & \ldots & \mathrm{res}_{P_n}(\omega_k) \end{pmatrix},$$

so

$$\begin{pmatrix} \overline{\omega_1} \\ \vdots \\ \overline{\omega_k} \end{pmatrix} = A \begin{pmatrix} \overline{\eta_1} \\ \vdots \\ \overline{\eta_n} \end{pmatrix}.$$

Let $l = g + \mu - 1$, then l is the dimension of $\Omega(-\mu P)$. Let $\beta_1, \ldots, \beta_l$ be a basis of $\Omega(-\mu P)$, then there exists a $(k \times l)$-matrix Y over $\mathbf{F}$ such that

$$\begin{pmatrix} \omega_1 \\ \vdots \\ \omega_k \end{pmatrix} - A \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix} = Y \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_l \end{pmatrix}.$$

Now $\mathrm{rank}(A) = k$ by Theorem 3, since $\deg(E-\mu P) \geq 2g-1$. Hence there exists an $(n \times l)$-matrix X over $\mathbf{F}$ such that

$$AX = Y$$

Thus

$$\begin{pmatrix} \omega_1 \\ \vdots \\ \omega_k \end{pmatrix} = A \left(\begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix} + X \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_l \end{pmatrix} \right).$$

Define

$$\varepsilon_i = \eta_i + \sum_{j=1}^{l} x_{ij}\beta_j \text{ for } i = 1, \ldots, n.$$

where x_{ij} is entry of matrix X in row i and column j. Then $\varepsilon_i \in \Omega(-P_i-\mu P)$ and $\mathrm{res}_{P_i}(\varepsilon_i) = 1$ and

$$\omega_i = \sum_{j=1}^{n} \mathrm{res}_{P_j}(\omega_i)\varepsilon_j, \text{ for } i = 1, \ldots, k.$$

Finally, for every $\omega \in \Omega(E-\mu P-D)$

$$\omega = \sum_{j=1}^{n} \mathrm{res}_{P_j}(\omega)\varepsilon_j.$$

by the linearity of res_{P_i} and since the corresponding statement is true for the basis $\omega_1, \ldots, \omega_k$ of $\Omega(E-\mu P-D)$. Clearly $(\varepsilon_i)_\infty = P_i + P$ if $\mu = 1$. □

Remark 8 In case $\mathcal{X}$ is the projective line, e.g. for classical Goppa codes with $n+1$ distinct rational points $P_1, \ldots, P_n, P_\infty$, where $P_i = (\alpha_i : 1)$ and $P_\infty = (1 : 0)$, and Goppa polynomial h, which is not zero at the points P_i, we can take for the differentials $\varepsilon_i = dX/(X - \alpha_i)$. For an arbitrary curve it is not so easy to find these differentials ε_i explicitly, see [22] in case of the Hermitian curve.

Definition 9 Let the assumptions be as in Proposition 11. For code $C_\Omega(D, E - \mu P)$, define the map

$$\varepsilon : \mathbf{F}^n \longrightarrow \Omega \quad \text{by} \quad \varepsilon(\boldsymbol{x}) = \sum_{i=1}^{n} x_i \varepsilon_i,$$

where $\varepsilon_1, \ldots, \varepsilon_n$ are given by Proposition 11.

Remark 9 The restriction of ε to $C_\Omega(D, E - \mu P)$ is the inverse map of α_Ω restricted to $\Omega(E - \mu P - D)$, as we will see in the following corollary.

Corollary 1 *Let the assumptions be as in Proposition 11. Let $\varepsilon_1, \ldots, \varepsilon_n$ be the differentials given by Proposition 11. Then*

$$\varepsilon(\mathbf{c}) \in \Omega(E - \mu P - D) \text{ if and only if } \mathbf{c} \in C_\Omega(D, E - \mu P).$$

Proof. By Proposition 11, there exist independent differentials $\varepsilon_1 \ldots, \varepsilon_n$ with $\varepsilon_i \in \Omega(-P_i - \mu P)$ and $\mathrm{res}_{P_i}(\varepsilon_i) = 1$, such that for every $\omega \in \Omega(E - \mu P - D)$

$$\omega = \sum_{i=1}^{n} \mathrm{res}_{P_i}(\omega) \varepsilon_i.$$

Let $\mathbf{c} \in C_\Omega(D, E - \mu P)$, then there exists an $\omega \in \Omega(E - \mu P - D)$ such that

$$\mathbf{c} = (\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega)),$$

so

$$\varepsilon(\mathbf{c}) = \sum_{i=1}^{n} \mathrm{res}_{P_i}(\omega) \varepsilon_i = \omega \in \Omega(E - \mu P - D).$$

Conversely, let $\varepsilon(\mathbf{c}) \in \Omega(E - \mu P - D)$, then one has $\mathrm{res}_{P_j}(\varepsilon(\mathbf{c})) = c_j$ for every $j = 1, \ldots, n$, so

$$\mathbf{c} = \alpha_\Omega(\varepsilon(\mathbf{c})) \in C_\Omega(D, E - \mu P)$$

by the definition of α_Ω. □

V The syndrome

In [12], [23] and [16], for the code $C_\Omega(D, G)$, the syndrome of $\boldsymbol{x} \in \mathbf{F}^n$ is defined by a map from $L(F)$ to $\mathbf{F}$, namely by $s(\boldsymbol{x}, f) = \sum_{i=1}^{n} x_i f(P_i) g(P_i)$, where $g \in L(G - F)$ and F is a divisor. But here we give a different definition of the syndrome of $\boldsymbol{x}$, namely as an element of $K_\infty(P)$, which is a generalization of the syndrome of classical Goppa codes. In this section, we will give the definition only for codes of the form $C_\Omega(D, E - \mu P)$. This is not a restriction since every geometric Goppa code is isometric with a code of this type, by the discussion in section III.

First we need some preparations.

Definition 10 [1, I.7] Let B be a divisor on $\mathcal{X}$. The rational functions f_1 and f_2 are said to be *congruent to each other modulo B under a set of places $\mathcal{O}$*, if we have $v_Q(f_1 - f_2) \geq v_Q(B)$ for every $Q \in \mathcal{O}$. We shall write

$$f_1 \equiv_{\mathcal{O}} f_2 (\text{mod } B).$$

In particular,
1) If $\mathcal{O}$ is the set of all places of $\mathcal{X}$, then we write $f_1 \equiv f_2 (\text{mod } B)$;
2) If $\mathcal{O}$ is the support of a divisor E on $\mathcal{X}$, then we write $f_1 \equiv_E f_2 (\text{mod } B)$.
3) If $B = (f)$, where f is a rational function, then we write $f_1 \equiv_{\mathcal{O}} f_2 (\text{mod } f)$.

Lemma 5 *Let $\langle h \rangle$ be the principal ideal of $K_\infty(P)$ generated by $h \in K_\infty(P)$. Let $E = (h)_0$. Then*

$$\{f \in K_\infty(P) | f \equiv_E 0 \ ((mod \ \ h \ )\} = \langle h \rangle.$$

Therefore for $f \in K_\infty(P)$, $f \equiv_E 0$ $((mod \ \ h \ )$ if and only if there exists a $q \in K_\infty(P)$ such that $f = qh$, that is $f \equiv 0$ $((mod \ \ h \ )$ in the ring $K_\infty(P)$.

Proof. Let $f \in \langle h \rangle$, then there is a $q \in K_\infty(P)$ such that $f = qh$. Thus

$$v_Q(f) = v_Q(q) + v_Q(h) \geq v_Q(h) \text{ for } Q \in \text{supp}(E),$$

hence $f \equiv_E 0 (\text{mod } h)$ by definition.

Conversely, let $f \in K_\infty(P)$ and $f \equiv_E 0 (\text{mod } h)$. Then by the Division Theorem 2, there exist $q, r \in K_\infty(P)$ such that $f = qh + r$ where $r = 0$ or $\deg(r) \in \text{gap}(h)$. We claim $r = 0$, therefore $f \in \langle h \rangle$. If it is not true, then for every $Q \neq P$ we have

$$v_Q(r) = v_Q(f - qh) \geq \min\{v_Q(f), v_Q(q) + v_Q(h)\} \geq v_Q(h),$$

since if $Q \notin \text{supp}((h)_0)$ then $v_Q(h) = 0$ and if $Q \in \text{supp}(h)$ then $v_Q(f) \geq v_Q(h)$. So $r/h \in K_\infty(P)$ and $r/h \neq 0$. Thus $\deg(r) - \deg(h) = \deg(r/h)$ is not a gap of P, that is $r \notin \text{gap}(h)$ which is a contradiction. □

Definition 11 Let W be a divisor on $\mathcal{X}$ and P be a rational point on $\mathcal{X}$, such that P is not in the support of W. Define $K_\infty(P, W)$ by

$$K_\infty(P, W) = \{f \in K_\infty(P) | f = 0 \text{ or } f \equiv_W 0 (\text{mod } W)\}$$

Lemma 6 *$K_\infty(P, W)$ is an ideal in $K_\infty(P)$.*

Proof. Let $f_1, f_2 \in K_\infty(P, W)$, then for every $Q \in \text{supp}(W)$, we have $v_Q(f_i) \geq v_Q(W)$ for $i = 1, 2$, so

$$v_Q(f_1 + f_2) \geq \min\{v_Q(f_1), v_Q(f_2)\} \geq v_Q(W).$$

Let $f \in K_\infty(P, W)$ and $h \in K_\infty(P)$, then for every $Q \in \text{supp}(W)$, we have $v_Q(f) \geq -v_Q(W)$ and $v_Q(h) \geq 0$, since $Q \neq P$. Hence $v_Q(fh) \geq v_Q(W)$. Therefore $fh \in K_\infty(P, W)$, so $K_\infty(P, W)$ is an ideal in $K_\infty(P)$. □

Proposition 12 *Let P be a place not in $\{P_1, \ldots, P_n\}$. Let E be an effective divisor. Then there exists a differential form η such that*

$$\text{supp}((\eta)_0) \subseteq \{P\} \text{ and } \text{supp}((\eta)) \cap (\{P_1, \ldots, P_n\} \cup \text{supp}(E)) = \emptyset,$$

If moreover $g > 1$, then

$$\text{supp}((\eta)_0) = \{P\}.$$

Proof. Suppose $\mathrm{supp}(E) = \{Q_1, \ldots, Q_m\}$. Let ω' be any nonzero differential form. By the independence of valuations, see [1, p. 11], there exists a rational function f_0 such that $v_P(f_0) = -v_P(\omega')$, $v_{P_i}(f_0) = -v_{P_i}(\omega')$ for $i = 1, \ldots, n$ and $v_{Q_i}(f_0) = -v_{Q_i}(\omega')$ for $i = 1, \ldots, m$. Define $\omega = f_0\omega'$, then $\omega \neq 0$ and

$$\mathrm{supp}((\omega)) \cap \{P, P_1, \ldots, P_n, Q_1, \ldots Q_m\} = \emptyset.$$

Now by Proposition 6, there exists an $f \in K_\infty(P)$ such that $(f)_{\mathcal{O}} = (\omega)_0$, where $\mathcal{O} = \mathrm{supp}((\omega)_0)$. Define $\eta = \omega f^{-1}$, then $\eta \neq 0$ and $(\eta) = (\omega) - (f) \leq -v_P(f)P$. Hence $\mathrm{supp}((\eta)_0) \subseteq \{P\}$ and $\mathrm{supp}((\eta)) \cap \{P_1, \ldots, P_n, Q_1, \ldots, Q_m\} = \emptyset$. If $g > 1$, then $2g - 2 > 0$, hence $(\eta)_0 \neq 0$, so $\mathrm{supp}((\eta)_0) = \{P\}$ and $\mathrm{supp}((\eta)_\infty) \cap (\{P, P_1, \ldots, P_n\} \cup \mathrm{supp}(E)) = \emptyset$. □

The following three examples give such an η explicitly with the additional property $\mathrm{supp}(\eta) = (2g-2)P$.

Example 4 The projective line $\mathbf{P}^1$ over $\mathbf{F}$, see Example 1.

If $P_\infty = (1:0)$ and $\eta = \mathrm{d}X$, then $\eta = (-X^2)\mathrm{d}(1/X)$. Hence $(\eta) = -2P_\infty$. If $P = (\alpha : 1)$ and $\eta = \mathrm{d}(1/(X-\alpha))$, then $(\eta) = -2P$.

Example 5 Hermitian Curve $H(q)$, see Example 2.

If $\eta = dx$, then $(\eta) = (2g-2)P$, see [24, Satz 1 (f)]

Example 6 Let $\mathcal{X}(l, q)$ be the curve as in Example 3.

The genus of this curve is $\{\sum_{i=1}^{l-1} q^{l+1-i}(q+1)^{i-1} - (q+1)^{l-1} + 1\}/2$ and this curve goes through all the q^l places of degree one, outside the hyperplane with equation $x_0 = 0$. Let $y_i = X_i/X_0$ for $i = 1 \ldots, l-1$, then

$$y_i^{q+1} - y_i^2 + y_{i+1} - y_{i+1}^q = 0 \text{ for } i = 1, \ldots, l-1.$$

The number $2g-1$ is a gap of $\tilde{P}_\infty$, see [17]. Thus there exists an $\eta \in \Omega$ such that $(\eta) = (2g-2)\tilde{P}_\infty$ by [18, Theorem 4.4.1] and [20, Lemma 1.1].

Remark 10 All these examples have the property that there exists a differential with support concentrated at at most one place. Other examples are rational, elliptic and hyperelliptic curves, see [18]. See Delgado [2] and Sathaye [20] for a caracterization of such curves. It would be interesting to know how big the class of such curves is, in particular whether there exists a family of curves such that the ratio of the number of rational points divided by the genus does not tend to zero, whereas the number of rational points tends to infinity.
Over an algebraically closed field of characteristic zero the situation is as follows. The moduli variety M_g, parametrizing all isomorphism classes of curves of genus g, has dimension $3g-3$, if $g > 1$. The subvariety P_g of M_g, of curves with a differential with support at one point, has dimension $2g-1$, see [19].
In the following we give an example of a curve without such a differential. The Klein quartic in characterisic two is also such a curve.

Example 7 A curve of genus 3, which is not hyperelliptic, has a plane model of degree 4. Effective canonical divisors are intersection divisors of this plane curve with a line. So there exists a differential η such that $(\eta) = 4P$ if and only if the plane model has a tangent line, which intersects the curve in P with multiplicity 4. The plane curve $\mathcal{X}$ defined over $GF(2)$

with equation: $XY(X+Y)(X+Z)+XZ^2(X+Z)+Y^2Z(Y+Z)=0$, see [17], has not such a differential. In fact, this curve has seven places of degree one, say $P_1, P_2, \ldots, P_7$. Every line L in $\mathbf{P}^2$, defined over $GF(2)$, has intersection $L.\mathcal{X} = 2P_i + P_j + P_k$, where i, j and k are mutually different. Therefore there does not exist a differential form such that its divisor is $(2g-2)P$ for some point P on $\mathcal{X}$.

Theorem 4 *Let P be a rational point not in $\{P_1, \ldots, P_n\}$. Let E be an effective divisor and μ a positive integer, such that $\deg(E - \mu P) \geq 2g-1$. Then by the results of the previous sections and the above proposition, we have the following conclusions:*
1) (Proposition 6). There exists an $h \in K_\infty(P)$, such that $(h)_{\mathcal{E}} = E$, where $\mathcal{E} = \mathrm{supp}(E)$.
2) (Proposition 11). There exist n differentials, namely $\varepsilon_1, \ldots, \varepsilon_n$, such that $\varepsilon_i \in \Omega(-P_i - \mu P)$ and $\mathrm{res}_{P_i}(\varepsilon_i) = 1$ for $i = 1, \ldots, n$. Moreover, for every $\omega \in \Omega(E - \mu P - D)$,

$$\omega = \sum_{i=1}^{n} \mathrm{res}_{P_i}(\omega)\varepsilon_i.$$

3) (Proposition 12). There exists a differential η, such that $(\eta)_0 = lP$ and

$$\mathrm{supp}((\eta)_\infty) \cap (\{P, P_1, \ldots, P_n\} \cup \mathrm{supp}(E)) = \emptyset.$$

Definition 12 The syndrome of the code $C_\Omega(D, E - \mu P)$ is defined by the map S from $\mathbf{F}^n$ to $\mathbf{F}(\mathcal{X})$, such that for every $\boldsymbol{x} \in \mathbf{F}^n$,

$$S(\boldsymbol{x})\eta = \sum_{i=1}^{n} x_i \frac{h(P_i) - h}{h(P_i)} \varepsilon_i.$$

$S(\boldsymbol{x})$ is called *the syndrome of* $\boldsymbol{x}$.

Remark 11 . The syndrome is well defined, since for every differential σ on $\mathcal{X}$ there is a unique $s \in \mathbf{F}(\mathcal{X})$ such that $\sigma = s\eta$. It follows immediately from the definition that S is a linear map over $\mathbf{F}$.

Proposition 13 *For every $\boldsymbol{x} \in \mathbf{F}^n$,*

$$S(\boldsymbol{x}) \in K_\infty(P, W),$$

where $W = (\eta)_\infty$.

Proof. For every $i = 1, \ldots n$, we have

$$v_Q(\frac{h(P_i) - h}{h(P_i)}\varepsilon_i) \geq 0 \text{ if } Q \notin \{P, P_i\}$$

and

$$v_{P_i}(\frac{h(P_i) - h}{h(P_i)}\varepsilon_i) \geq 1 + v_{P_i}(\varepsilon_i) \geq 0,$$

since $h \in K_\infty(P)$ and $\varepsilon_i \in \Omega(-P_i - \mu P)$. Thus $v_Q(S(\boldsymbol{x})\eta) \geq 0$ for $Q \neq P$. Hence

$$v_Q(S(\boldsymbol{x})) = v_Q(S(\boldsymbol{x})\eta) - v_Q(\eta) \geq -v_Q(\eta) \text{ for } Q \neq P.$$

Therefore $S(\boldsymbol{x}) \in K_\infty(P, W)$. □

The name syndrome $S(\boldsymbol{x})$ of $\boldsymbol{x}$ is justified by the following theorem.

Theorem 5 *Under the assumptions of Theorem 4 we have that*

$$\mathbf{c} \in C_\Omega(D, E - \mu P) \text{ if and only if } S(\mathbf{c}) \equiv_E 0 (mod\ h).$$

If moreover $E = (h)_0$, *then*

$$\mathbf{c} \in C_\Omega(D, E - \mu P) \text{ if and only if } S(\mathbf{c}) \equiv 0 (mod\ h) \text{ in } K_\infty(P).$$

Proof. If $\mathbf{c} \in C_\Omega(D, E - \mu P)$, then there is an $\omega \in \Omega(E - \mu P - D)$ such that

$$\mathbf{c} = (\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega)),$$

so

$$S(\mathbf{c})\eta = \sum_{i=1}^{n} \mathrm{res}_{P_i}(\omega) \frac{h(P_i) - h}{h(P_i)} \varepsilon_i = \omega - h \sum_{i=1}^{n} \frac{c_i}{h(P_i)} \varepsilon_i,$$

by Proposition 11. Let $Q \in \mathrm{supp}(E)$, then:
i) $v_Q(\omega) \geq v_Q(E) = v_Q(h)$;
ii) $v_Q(h \sum_{i=1}^{n} c_i \varepsilon_i / h(P_i)) \geq v_Q(h)$;
iii) $v_Q(\eta) = 0$ since $\mathrm{supp}((\eta)) \cap \mathrm{supp}(E) = \emptyset$.
Hence

$$v_Q(S(\mathbf{c})) = v_Q(\omega - h \sum_{i=1}^{n} \frac{c_i}{h(P_i)} \varepsilon_i) - v_Q(\eta) \geq v_Q(h).$$

Thus $S(\mathbf{c}) \equiv_E 0 (\mathrm{mod}\ h)$.

Conversely, suppose $\mathbf{c} \in \mathbf{F}^n$, then

$$S(\mathbf{c})\eta = \varepsilon(\mathbf{c}) - h \sum_{i=1}^{n} \frac{c_i}{h(P_i)} \varepsilon_i.$$

Let $S(\mathbf{c}) \equiv_E 0 (\mathrm{mod}\ h)$. Then for $Q \in \mathrm{supp}(E)$,

$$v_Q(\varepsilon(\mathbf{c})) \geq \min\{v_Q(S(\mathbf{c})) + v_Q(\eta), v_Q(h) + v_Q(\sum_{i=1}^{n} \frac{c_i}{h(P_i)} \varepsilon_i)\} \geq v_Q(h).$$

For all other places, we have $\sum_{Q \notin \mathrm{supp}(E)} v_Q(\varepsilon(\mathbf{c})) \geq -D - \mu P$. Combining those two, we have

$$\varepsilon(\mathbf{c}) \in \Omega(E - \mu P - D).$$

Hence $\mathbf{c} = \alpha_\Omega(\varepsilon(\mathbf{c})) \in C_\Omega(D, E - \mu P)$, by Corollary 1. If moreover $E = (h)_0$, then the conclusion follows from the above and Lemma 5. □

VI Decoding by solving the key congruence

Let P be an extra place, that is not in $\{P_1, \ldots, P_n\}$. Let E be an effective divisor with disjoint support with D and P, Let μ be a positive integer, such that $\deg(E - \mu P) \geq 2g - 1$. By the discussion in section III, we know that, to decode all geometric Goppa codes it is sufficient to give a decoding algorithm for codes of the form $C_\Omega(D, E - \mu P)$.

Definition 13 Let $S(\boldsymbol{x})$ be the syndrome of $\boldsymbol{x} \in \mathbf{F}^n$ with respect to (D, E, P). Let $h \in K_\infty(P)$ and $\eta \in \Omega$ be given in Theorem 4 for the code $C_\Omega(D, E - \mu P)$. Let $W = (\eta)_\infty$ and $l = \deg(\eta)_0$.
1) If $f \in K_\infty(P)$ and $r \in K_\infty(P, W)$ are such that

$$fS(\boldsymbol{x}) \equiv_E r (\text{mod } h),$$

then we say that (f, r) satisfies the *key congruence* of $\boldsymbol{x}$ with respect to (D, E, P).
If moreover

$$\deg(r) - \deg(f) \leq l + \mu,$$

then the pair (f, r) is called a *valid* solution of the key congruence.
If furthermore (f, r) is a valid solution and $\deg(f)$ is minimal among all the degrees of f' such that (f', r') is a valid solution, then (f, r) is called a *minimal* valid solution of the key congruence.
2) If $E = (h)_0$ and $f \in K_\infty(P)$ and $r \in K_\infty(P, W)$ such that

$$fS(\boldsymbol{x}) = r + qh \quad \text{for some} \quad q \in K_\infty(P, W),$$

then we say that (f, r) satisfies the *key equation* of $\boldsymbol{x}$ with respect to (D, E, P).
Similarly as in 1) we define what a (minimal) valid solution of the key equation is.

Definition 14 The *Clifford defect* of the pair (E, P) is defined by

$$s = \max\{\frac{\deg(E - kP)}{2} - (l(E - kP) - 1) | k \in \mathbf{N}\}.$$

For the details of the Clifford defect we refer to Duursma [4].

Remark 12 Suppose g is the genus of the curve used. Then it is easy to see that

$$s = \max\{\frac{\deg(E - kP)}{2} - (l(E - kP) - 1) | \deg(E) - 2g + 1 \leq k \deg(P) \leq \deg(E)\},$$

and $s \leq g/2$.

Definition 15 Let I be a subset of $\{1, \ldots, n\}$. Let $Q = \sum_{i \in I} P_i$. Define

$$K_I(P) = \bigcup_{k \in \mathbf{N}} L(kP - Q).$$

Let b_I be the smallest integer for which $l(b_I P - Q) \neq 0$.

Proposition 14 *Let $\#(I) \leq (d^* - \deg(P))/2 - s$, where $d^* = deg(E) - \mu \deg(P) - 2g + 2$ (see Theorem 3) and s is the Clifford defect of (E, P). Then*

$$\Omega(E - (\mu + b_I)P - Q) = \{0\},$$

where $Q = \sum_{i \in I} P_i$.

Proof. Let t be the number of elements of I. Assume

$$\Omega(E-(\mu+b_I)P-Q)\neq\{0\}.$$

Then there exists a nonzero differential ω and an effective divisor E^* such that

$$(\omega)-E+(\mu+b_I)P+Q\sim E^*,$$

hence

$$\deg(E^*)=2g-2-\deg(E)+(\mu+b_I)\deg(P)+t.$$

Therefore

$$(b_I-1)P-Q\sim K-E+(\mu+2b_I-1)P-E^*,$$

where K represents the canonical divisor class. Now by the assumption of b_I we have

$$l(K-E+(\mu+2b_I-1)P-E^*)=0,$$

and therefore

$$\deg(E^*)\geq l(K-E+(\mu+2b_I-1)P).$$

By the Riemann-Roch Theorem

$$l(K-E+(\mu+2b_I-1)P)=l(E-(\mu+2b_I-1)P)-\deg(E)+(\mu+2b_I-1)\deg(P)+g-1.$$

Hence by the above and the definitions of t and the Clifford defect s, we have

$$\begin{aligned}\deg(E^*) &\geq (\deg(E)-(\mu+2b_I-1)P)/2-s+1\\ &\quad -\deg(E)+(\mu+2b_I-1)\deg(P)+g-1\\ &\geq t-\deg(E)+2g-2+(\mu+b_I)\deg(P)+1\\ &= \deg(E^*)+1,\end{aligned}$$

which is a contradiction. □

Theorem 6 (**Decoding Theorem**) *Let $\boldsymbol{x}\in\mathbf{F}^n$ with $\boldsymbol{x}=\boldsymbol{c}+\boldsymbol{e}$, where $\boldsymbol{c}$ is a code word of $C_\Omega(D,E-\mu P)$ and $\boldsymbol{e}$ is an error vector. Let η be given by Theorem 4. Then*

Existence: There exists a valid solution (f,r) of the key congruence of $\boldsymbol{x}$ with respect to (D,E,P), such that

$$\frac{r}{f}\eta\in\Omega(-D-\mu P)\quad \textit{and}\quad \alpha_\Omega(\frac{r}{f}\eta)=\boldsymbol{e}.$$

Uniqueness: Let $t=(d^*-\deg(P))/2-s$, where d^* is the designed minimun distance and s is Clifford defect of this code. Suppose $wt(\boldsymbol{e})\leq t$. If (f,r) is a minimal valid solution of the key congruence of $\boldsymbol{x}$ with respect to (D,E,P), then

$$\frac{r}{f}\eta\in\Omega(-D-\mu P)\quad \textit{and}\quad \alpha_\Omega(\frac{r}{f}\eta)=\boldsymbol{e}.$$

Proof. Let $I = \{i | e_i \neq 0, 1 \leq i \leq n\}$, where $(e_1, \ldots, e_n) = \boldsymbol{e}$.
Existence: The vector space of differentials on $\mathcal{X}$ is one dimensional over $\mathbf{F}(\mathcal{X})$, so η is a basis of Ω. Hence for every $i \in \{1, \ldots, n\}$, there exists an $u_i \in \mathbf{F}(\mathcal{X})$ such thst $\varepsilon_i = u_i\eta$, where ε_i, for $i = 1, \ldots, n$, are given by Theorem 4. Therefore by the definitions of η and ε_i, one has

1) $v_P(u_i) = v_P(\varepsilon_i) - v_P(\eta) \geq -l - \mu$;
2) $v_{P_j}(u_i) = v_{P_j}(\varepsilon_i) - v_{P_j}(\eta) = -\delta_{ij}$, where δ_{ij} is 1 if $i = j$ and 0 otherwise.
3) $v_R(u_i) = v_R(\varepsilon_i) - v_R(\eta) \geq 0$, if $R \notin \{P_1, \ldots, P_n, P\}$.

Let f_0 be a nonzero element of $K_I(P)$, then $v_{P_i}(f_0) \geq 1$ and therefore $f_0 u_i \in K_\infty(P)$ for every $i \in I$. Define $r_0 = f_0 \sum_{i \in I} e_i u_i$. Then $r_0 \in K_\infty(P)$ and $(r_0/f_0)\eta = \varepsilon(\mathbf{e})$, so $\alpha_\Omega((r_0/f_0)\eta) = \boldsymbol{e}$, and also

$$v_R(r_0) = v_R(f_0) + v_R(\varepsilon(\mathbf{e})) - v_R(\eta) \geq -v_R(\eta),$$

for all places R not in $\{P_1, \ldots, P_n, P\}$, thus $r_0 \in K_\infty(P, W)$.

Now by the definition of the syndrome we have

$$\begin{aligned} f_0 S(\boldsymbol{x})\eta &= f_0 \sum_{i=1}^{n} x_i \frac{h(P_i) - h}{h(P_i)} \varepsilon_i \\ &= f_0 \varepsilon(\mathbf{e}) + f_0 S(\mathbf{c})\eta - f_0 h \sum_{i \in I} \frac{e_i}{h(P_i)} \varepsilon_i \\ &= (r_0 + f_0 S(\boldsymbol{c}) - f_0 h \sum_{i \in I} \frac{e_i}{h(P_i)} u_i)\eta, \end{aligned}$$

where $h \in K_\infty(P)$ is given by Theorem 4, that is $(h)_0 = E$. Thus $f_0 S(\boldsymbol{x}) \equiv_E r_0 (\mathrm{mod}\ h)$ since $S(\boldsymbol{c}) \equiv_E 0 (\mathrm{mod}\ h)$ by Theroem 5, and

$$\deg(r_0) - \deg(f_0) = -v_P(r_0) + v_P(f_0) = -v_P(\varepsilon(\boldsymbol{e})) + v_P(\eta) \leq l + \mu.$$

This proves the existence.

Uniqueness: Now $wt(\boldsymbol{e}) \leq t$, hence $\#(I) \leq t$. By the assumption we have $\deg(f) \leq b_I$. Let $Q = \sum_{i \in I} P_i$. We claim that

$$r\eta - f\varepsilon(\boldsymbol{e}) \in \Omega(E - (\mu + b_I)P - Q),$$

and therefore $r\eta - f\varepsilon(\boldsymbol{e}) = 0$, by Proposition 14. Thus

$$(r/f)\eta = \varepsilon(\boldsymbol{e}) \in \Omega(-D - \mu P) \quad \text{and} \quad \alpha_\Omega((r/f)\eta) = \boldsymbol{e}.$$

Now we prove our claim. Let us consider the valuation of $r\eta - f\varepsilon(\boldsymbol{e})$ at every place of the curve.

Since $r \in K_\infty(P, W)$, we have

$$v_R(r\eta - f\varepsilon(\boldsymbol{e})) \geq 0 \tag{1}$$

for every $R \notin \{P_1, \ldots, P_n, P\}$. Now look at the valuation of $r\eta - f\varepsilon(\boldsymbol{e})$ at R such that $R \in \mathrm{supp}(E)$. First by the assumption, we have $v_R(fS(\boldsymbol{x})\eta - r\eta) \geq v_R(h)$, that is

$$v_R(r\eta - f\varepsilon(\boldsymbol{e}) - f[S(\boldsymbol{x})\eta - \varepsilon(\boldsymbol{e})]) \geq v_R(h).$$

Moreover, we have

$$\begin{aligned}(S(\boldsymbol{x})\eta - \varepsilon(\boldsymbol{e})) &= \sum_{i=1}^{n}(x_i - hx_i/h(P_i) - e_i)\varepsilon_i \\ &= \varepsilon(\boldsymbol{c}) - h\sum_{i=1}^{n} x_i/h(P_i)\varepsilon_i.\end{aligned}$$

Hence $v_R(f(S(\boldsymbol{x})\eta - \varepsilon(\boldsymbol{e})) \geq v_R(h)$ since $\varepsilon(\boldsymbol{c}) \in \Omega(E - \mu P - D)$. Therefore we can conclude that, for every $R \in \mathrm{supp}(E)$,

$$v_R(r\eta - f\varepsilon(\boldsymbol{e})) \geq v_R(h). \tag{2}$$

For the rational points P_i, $i = 1, \ldots, n$, we have

$$v_{P_i}(r\eta - f\varepsilon(\boldsymbol{e})) \geq \begin{cases} -1 & \text{if } i \in I, \\ 0 & \text{if } i \notin I. \end{cases} \tag{3}$$

At last, we have

$$\begin{aligned}v_P(r\eta - f\varepsilon(\boldsymbol{e})) &= v_P(f[(r/f)\eta - \varepsilon(\boldsymbol{e})]) \\ &\geq -\deg(f) + \min\{-\deg(r) + \deg(f) + l, -\mu\} \\ &\geq -b_I - \mu, \end{aligned} \tag{4}$$

since $\deg(r) - \deg(f) \leq l + \mu$.

Combining (1), (2), (3) and (4) gives

$$r\eta - f\varepsilon(\boldsymbol{e}) \geq E - Q - (b_I + \mu)P,$$

hence

$$r\eta - f\varepsilon(\boldsymbol{e}) \in \Omega(E - (b_I + \mu)P - Q).$$

This proves our claim. □

VII Decoding codes isometric with $C_\Omega(D, mP)$

In this section we assume that the code length is smaller than the number of rational points, so there exists a rational point P not in $\{P_1, \ldots, P_n\}$. We know that $C_\Omega(D, mP)$ is isometric with $C_\Omega(D, (h)_0 - \mu P)$ for some $h \in K_\infty(P)$. Hence it is sufficient to give a decoding theorem of the code $C_\Omega(D, (h)_0 - \mu P)$. First let us look at the details of the Clifford defect of this class.

Proposition 15 *The Clifford defect s of $((h)_0), P)$ is*

$$s = \max\{k/2 - l(kP) + 1 | 0 \leq k \leq 2g - 1\},$$

Proof. Since $h \in K_\infty(P)$, hence $(h)_0 \sim \deg(h)P$. Therefore $l((h)_0 - kP) = l((\deg(h) - k)P)$. Thus by the definition of Clifford defect we immediately have the desired result. □

Proposition 16 *Let $\mathcal{H}(q)$ be the Hermitian curve over $\mathbf{F} = GF(q^2)$ with the function field $\mathbf{F}(x,y)$, where $x^{q+1} = y^q + y$. Let P be the common pole of x and y (for the details of this curve we refer to [24]). Then the Clifford defect of $((h)_0), P)$ is*

$$s = \begin{cases} (q-1)^2/8 + 1/2 & \text{if } q \equiv 1(mod\ 2); \\ (q-2)^2/8 + 1/2 & \text{if } q \equiv 0(mod\ 2). \end{cases}$$

Proof. See also Duursma [4]. It is easy to see that the non-gaps of P between 0 to $2g-1$ are

$$iq + j(q+1), 0 \le i \le q, 0 \le j \le q - i - 2,$$

and the gaps of P are

$$j(q+1)+1, \ldots, (j+1)q - 1, 0 \le j \le q-2.$$

For the details of this conclusion we refer to [22]. Then we have

$$l((iq + j(q+1))P) = \frac{(i+j)(i+j+1)}{2} + j + 1,$$

where $0 \le i \le q$ and $0 \le j \le q - i - 2$, and

$$l((j(q+1)+k)P) = l((j+1)qP) - 1,$$

for $1 \le k \le q - j - 1$, where $0 \le j \le q-2$. Let $s(k) = k/2 - l(kP) + 1$. It is easy to prove that

$$s(iq + j(q+1)) \le \begin{cases} (q-1)^2/8 & \text{if } q \equiv 1(\text{mod } 2); \\ (q-2)^2/8 & \text{if } q \equiv 0(\text{mod } 2), \end{cases}$$

and the equality holds if

$$(i,j) = \begin{cases} ((q-1)/2, 0) \text{ if } q \equiv 1(\text{mod } 2); \\ ((q-2)/2, 0) \text{ if } q \equiv 0(\text{mod } 2). \end{cases}$$

Furthermore

$$s(j(q+1)+k) \le s((j+1)q) + \frac{1}{2},$$

where $l \le q - j - 1$, and the equlity holds if $l = q - j - 1$. Therefore our proposition follows immediately from the above two inequalities. □

As a special case of the Decoding Theorem in section VI, the following theorem gives method to decode geometric Goppa codes isometric with $C_\Omega(D, mP)$.

Theorem 7 *Let $\boldsymbol{x} \in \mathbf{F}^n$ with $\boldsymbol{x} = \boldsymbol{c} + \boldsymbol{e}$, where $\boldsymbol{c}$ is a code word of $C_\Omega(D, (h)_0 - \mu P)$ and $\boldsymbol{e}$ is an error vector. Let η be given by Theorem 4. Then*

Existence: There exists a valid solution (f, r) of the key equation of $\boldsymbol{x}$ with respect to $(D, (h)_0, P)$, such that

$$\frac{r}{f}\eta \in \Omega(-D - \mu P) \quad \text{and} \quad \alpha_\Omega(\frac{r}{f}\eta) = \boldsymbol{e}.$$

Uniqueness: Let $t = (d^* - 1)/2 - s$, where d^* is the designed minimun distance and s is Clifford defect of this code. Suppose $wt(\boldsymbol{e}) \leq t$. If (f, r) is a minimal valid solution of the key equation of $\boldsymbol{x}$ with respect to $(D, (h)_0, P)$, then

$$\frac{r}{f}\eta \in \Omega(-D - \mu P) \quad \textit{and} \quad \alpha_\Omega(\frac{r}{f}\eta) = \boldsymbol{e}.$$

Proof. By using Lemma 5, this theorem is a special case of Theorem 6, since $\deg(P) = 1$. □

Remark 13 By the above theorem, we see that we can decode $C_\Omega(D, mP)$ if we can solve the key equation. In [21], Shen gives an algorithm for solving the key equation using the subresultant sequence, a generalization of the Euclidean algorithm, which corrects and generalizes the method given in [18], so that the algorithm can correct upto $(d^* - 1)/2 - s$ errors with complexity $O(n^3)$. For the Hermitian curves $\mathcal{H}(q)$, Shen [22] gives a more effecient algorithm for solving the key equation, which is a generalization of the Berlekamp-Massey decoding algorithm, following ideas of Sakata.

VIII This method may not correct more than $(d^* - 1)/2 - s$ errors

Let $\mathcal{H}(3)$ be the Hermitian curve $U^4 + V^4 + W^4 = 0$ over $\mathbf{F} = GF(9)$. Then the function field of $\mathcal{H}(3)$ is $\mathbf{F}(x, y)$, where the defining equation is $x^4 = y^3 + y$. The the genus of this curve is 3, see [24]. Suppose α is a primitive element of $GF(9)$, then

$$\alpha^2 = \alpha + 1, \alpha^3 = 2\alpha + 1, \alpha^4 = 2, \alpha^5 = 2\alpha, \alpha^6 = 2\alpha + 2, \alpha^7 = \alpha + 2, \alpha^8 = 1.$$

All the rational points of $\mathcal{H}$ are the following,

(1) a point at infinity P;

(2)

$$\begin{array}{lllll}
P_0 = (0,0), & P_1 = (\alpha,1), & P_2 = (\alpha^3,1), & P_3 = (\alpha^5,1), & P_4 = (\alpha^7,1) \\
P_5 = (\alpha^2,\alpha), & P_6 = (2,\alpha), & P_7 = (\alpha^6,\alpha), & P_8 = (1,\alpha), & P_9 = (0,\alpha^2), \\
P_{10} = (\alpha^2,\alpha^3), & P_{11} = (2,\alpha^3), & P_{12} = (\alpha^6,\alpha^3), & P_{13} = (1,\alpha^3), & P_{14} = (\alpha^2,2), \\
P_{15} = (2,2), & P_{16} = (\alpha^6,2), & P_{17} = (1,2), & P_{18} = (\alpha,\alpha^5), & P_{19} = (\alpha^3,\alpha^5), \\
P_{20} = (\alpha^5,\alpha^5), & P_{21} = (\alpha^7,\alpha^5), & P_{22} = (0,\alpha^6), & P_{23} = (\alpha,\alpha^7), & P_{24} = (\alpha^3,\alpha^7), \\
P_{25} = (\alpha^5,\alpha^7), & P_{26} = (\alpha^7,\alpha^7), & & &
\end{array}$$

and $K_\infty(P) = \mathbf{F}[x, y]$, for the details we refer to [22] and [24].

Let $D = \sum_{i=1}^{26} P_i$ and $E = (y^4)_0 = 16P_0$. In this section we will consider the code $C_\Omega(D, E-P)$ which is isometric to the code $C_\Omega(D, 15P)$. Denote $P_i = (\alpha_i, \beta_i)$ for $i = 1, \ldots, 26$ and let

$$\varepsilon_i = \{\frac{(y - \beta_i)^2 + 1}{x - \alpha_i} - \sum_{k=0}^{1}\sum_{\nu=0}^{k} \alpha_i^{k+2}\beta_i^{-(\nu+1)} x^{1-k} y^\nu\} dx,$$

where $i = 1, \ldots, 26$, then we have $(\varepsilon_i)_\infty = P_i + P$ and $\omega = \sum_{i=1}^{26} \mathrm{res}_{P_i}(\omega)\varepsilon_i$ for every $\omega \in C_\Omega(D, E - P)$. Let $\eta = dx$. Hence the syndrome of $\boldsymbol{x} \in \mathbf{F}^{26}$ is

$$S(\boldsymbol{x}) \equiv \sum_{i=1}^{26} x_i\beta_i^{-1}(\sum_{k=0}^{3}\sum_{j=0}^{3} \alpha_i^k\beta_i^j x^{3-k}y^{3-j} + \sum_{k=0}^{1}\sum_{\nu=0}^{k} \alpha_i^{k+2}\beta_i^{3-\nu}x^{1-k}y^\nu) (\mathrm{mod}\ y^4)$$

(for the details we refer to [22]).

By Theorem 3 and Proposition 16, we know that the designed minimum distance is $d^* = 11$ and the Clifford defect is 1. Therefore one can correct up to 4 errors by solving the key equation, see Theorem 7. The following example shows that one can not always correct 5, which is equal to $(d^* - 1)/2$, errors.

Example 8 Suppose the error vector $\boldsymbol{e}$ has nonzero values at the locations P_1, P_2, P_3, P_4 and P_9 (for the reason of this choice we refer to [4, Proposition 5]), hence we can suppose the received word is $\boldsymbol{x} = (1111000010 \cdots 0)$. Then the syndrome of $\boldsymbol{x}$ is

$$\begin{aligned} S(\boldsymbol{x}) &\equiv \sum_{i=1}^{4}(\sum_{k=0}^{3}\sum_{j=0}^{3}\alpha_i^k x^{3-k}y^{3-j} + \sum_{k=0}^{1}\sum_{\nu=0}^{k}\alpha_i^{k+2}x^{1-k}y^{\nu}) \\ &+ x^3y^3 + \alpha^2x^3y^2 + \alpha^4x^3y + \alpha^6x^3 (\mathrm{mod}\ y^4) \\ &= 2x^3y^3 + \alpha^7x^3y^2 + 2\alpha x^3 (\mathrm{mod}\ y^4). \end{aligned} \tag{5}$$

Furthermore we have

$$\begin{aligned} xS(\boldsymbol{x}) &\equiv (y^3 + y)(2y^3 + \alpha^7y^2 + 2\alpha)(\mathrm{mod}\ y^4) \\ &\equiv 2y^3 + 2\alpha y (\mathrm{mod}\ y^4); \end{aligned} \tag{6}$$

$$yS(\boldsymbol{x}) \equiv (\alpha^7x^3y^3 + 2\alpha x^3y)(\mathrm{mod}\ y^4); \tag{7}$$

$$x^2S(\boldsymbol{x}) \equiv 2xy^3 + 2\alpha xy (\mathrm{mod}\ y^4); \tag{8}$$

and

$$xyS(\boldsymbol{x}) \equiv 2\alpha y^2 (\mathrm{mod}\ y^4). \tag{9}$$

Now let $f = Ax^2 + By + Cx + D \neq 0$, where $A, B, C, D \in GF(9)$. Then

$$\begin{aligned} fS(\boldsymbol{x}) &\equiv B\alpha^7x^3y^3 + 2Bx^3y + 2Axy^3 + 2Axy + 2Cy^3 + \\ &\quad +2Cy + 2Dx^3y^3 + \alpha^7Dx^3y^2 + 2Dx^3 (\mathrm{mod}\ y^4) \end{aligned}$$

by (5),(6),(7),(8) and (9). Therefore, if there exists an $r \in K_\infty(P)$ such that

$$fS(\boldsymbol{x}) \equiv r (\mathrm{mod}\ y^4) \text{ and } \deg(r) - \deg(f) \leq 2g - 1 = 5,$$

then $A = B = C = D = 0$, which is a contradiction to $f \neq 0$.

Hence the minimal degree of f which satisfies $\deg(fS(\boldsymbol{x})(\mathrm{mod}\ y^4)) - \deg(f) \leq 2g-1 = 5$ is at least 7. But there exist at least two independent solutions, namely $f_1 = xy$ and $f_2 = xy - x$, where

$$f_1S(\boldsymbol{x}) \equiv 2\alpha y^2 (\mathrm{mod}\ y^4) \text{ and } f_2S(\boldsymbol{x}) \equiv y^3 + 2\alpha y^2 + \alpha y (\mathrm{mod}\ y^4).$$

Moreover, let $r_1 = 2\alpha y^2$, then

$$(res_{P_1}(\frac{r_1}{f_1}dx), \ldots, res_{P_{26}}(\frac{r_1}{f_1}dx)) \neq \boldsymbol{e}.$$

Hence, we conclude that by finding a minimal valid solution of the key equation, in particular by using the subresultant sequence [21], we may not get the right error vector $\boldsymbol{e}$ when $\mathrm{wt}(\boldsymbol{e}) > (d^* - 1)/2 - s$.

Acknowledgment

The authors would like to thank I.M. Duursma for his suggestion of correcting more errors.

References

[1] C. Chevalley, Introduction to the theory of algebraic functions in one variable, Math. Surveys VI, Providence, AMS 1951.

[2] F. Delgado, The symmetry of the Weierstrass generalized semigroups and affine embedding, Proc.Amer. Math. Soc. **108** (1990), 627-631.

[3] Y. Driencourt and J.F. Michon, Elliptic codes over fields of characteristic 2, J. Pure Appl. Algebra **45** (1987), 15-39.

[4] I.M. Duursma, Algebraic decoding using special divisors, preprint, to appear in IEEE Trans. Inform. Theory .

[5] D. Ehrhard, Decoding algebraic-geometric codes by solving a key equation, to appear in the Proceedings AGCT-3, Luminy, France, 1991, Springer Lect. Notes.

[6] W. Fulton, Algebraic curves, Benjamin, 1969.

[7] V.D. Goppa, Codes associated with divisors, Probl. Peredachi Inform. **13**(1) (1977), 33-39. Translation: Probl. Inform. Transmission **13** (1977), 22-26.

[8] V.D. Goppa, Codes on algebraic curves, Dokl. Akad. Nauk SSSR **259** (1981), 1289-1290. Translation: Soviet Math. Dokl. **24** (1981), 170-172.

[9] V.D. Goppa, Algebraico-geometric codes, Izv. Akad. Nauk SSSR **46** (1982), Translation: Math. USSR Izvestija **21** (1983), 75-91.

[10] V.D. Goppa, Codes and information, Russian Math. Surveys **39** (1984), 87-141.

[11] C.D. Jensen, Codes and geometry, Ph.D. Thesis, may 1991, Technical University of Denmark.

[12] J. Justesen, K.J. Larsen, H.Elbrønd Jensen, A. Havemose and T. Høholdt, Construction and decoding of a class of algebraic geometric codes, IEEE Trans. Inform. Theory IT-**35** (1989), 811-821.

[13] J. Justesen, K.J. Larsen, H.Elbrønd Jensen and T. Høholdt, Fast decoding of codes from algebraic plane curves, IEEE Trans. Inform. Theory IT-**38** (1992), 111-119.

[14] V.Yu. Krachkovskii, Decoding of codes on algebraic curves, preprint in Russian, 1988.

[15] J.H. van Lint and G. van der Geer , Introduction to coding theory and algebraic geometry, DMV Seminar **12**, Birkhauser Verlag, Basel Boston Berlin, 1988.

[16] R. Pellikaan, On a decoding algorithm for codes on maximal curves, IEEE Trans. Inform. Theory IT-**35** (1989), 1228-1232.

[17] R. Pellikaan, B.Z. Shen and G.J.M. Wee, Which linear codes are algebraic-geometric? IEEE Trans. Inform. Theory IT-**37** (1991), 583-602.

[18] S.C. Porter, Decoding codes arising from Goppa's construction on algebraic curves, Thesis, Yale University, dec. 1988.

[19] D.S. Rim and M.A. Vitulli, Weierstrass points and monomial curves, Journ. Algebra **48** (1977), 454-476.

[20] A. Sathaye, On planar curves, Amer. J. Math, **99** (1974), 1105-1135.

[21] B.-Z. Shen, Subresultant sequences on a Weierstrass algebra and an application to the decoding of geometric Goppa codes, preprint in Eindhoven University of Technology, May 1991.

[22] B.-Z. Shen, Codes from Hemitian curves and an iterative decoding algorithm, preprint Eindhoven University of Technology, June 1991.

[23] A. Skorobogatov and S. Vlăduţ, On the decoding of algebraic-geometric codes, IEEE Trans. Inform. Theory IT-**36** (1990), 1051-1060.

[24] H. Stichtenoth, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzablcharakteristik, teil 2, Arch. Math. **24** (1973), 615-631.

[25] H. Stichtenoth, A note on Hermitian codes over GF(q^2), IEEE Trans. Inform. Theory IT-**34** (1988), 1345-1348.

[26] H. Stichtenoth, On the automorphisms of geometric Goppa codes, J. Algebra **130** (1990), 113-121.

[27] H. J. Tiersma, Remarks on codes from Hermitian curves, IEEE Trans. Inform. Theory IT-**33** (1987), 605-609.

[28] M. A. Tsfasman, S. G. Vlăduţ and T. Zink, Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound, Math. Nachrichten **109** (1982), 21-28.

[29] M. Tsfasman and S. Vlăduţ, Algebraic-geomtric codes, Kluwer, Dordrecht, 1991.

[30] S.G. Vlăduţ, On the decoding of algebraic-geometric codes over $\mathbf{F}_q$ for $q \geq 16$, IEEE Trans. Inform. Theory IT-**36** (1990), 1461-1463.