Equality of geometric Goppa codes and equivalence of divisors

Carlos Munuera and Ruud Pellikaan *

Appeared in: Journ. Pure Appl. Algebra **90** (1993), 229-252.

Abstract

We give necessary and sufficient conditions for two geometric Goppa codes $C_L(D, G)$ and $C_L(D, H)$ to be the same. As an application we characterize self-dual geometric Goppa codes.

1 Introduction

Goppa used algebraic curves over finite fields to define linear codes, see [5, 6, 7]. Let $\mathcal{X}$ be a curve of genus g over a finite field $\mathbf{F}_q$ with q elements. If $\mathcal{X}$ has n rational points and L is a vector space of rational functions on $\mathcal{X}$, then one can define a q-ary code of wordlength n by evaluating the functions at the rational points. Usually one takes $L = L(G)$, where G is a divisor on $\mathcal{X}$, thus L is a vector space of rational functions with behaviour at poles and zeros prescribed by G. Such codes are called geometric Goppa or algebraic-geometric codes. If G and H are two divisors such that the difference is the principal divisor of a rational function which is 1 at the n rational points, then they define the same code. Xing [17] showed that the converse holds whenever $\deg(G) < n/2$ or $\deg(G) > n/2 + 2g - 2$. An immediate consequence of such a result gives a characterization of divisors defining a self-dual code. The question on self-dual codes was considered before by Driencourt, Michon, Stichtenoth and Xing, see [1, 2, 3, 4, 11, 12, 17], and also by Katsman and Tsfasman, see [16, p. 387]. The best result so far is that if $n > 6g - 4$, then G defines a self-dual code if and only if there exists a differential form η such that $(\eta) = 2G - D$ and η has simple poles and residue 1 at all the n rational points, see [17]. We will show that the assumption $n > 2g+2$ instead of $n > 6g-4$ is sufficient for the characterization to hold.

*The first author is with the University of Valladolid, Department of Applied Mathematics (ETS de Aquitectura), Avda Salamanca S/N, 47014 Valladolid, Castilla Spain, email cmunuera@cpd.uva.es and the last author is with the Eindhoven University of Technology, Department of Mathematics and Computing Science, P.O. Box 513, MB 5600 Eindhoven, The Netherlands, email ruudp@win.tue.nl

In the paper of Xing it is also assumed that the divisor used has degree m such that $2g-1 < m < n-1$. We wanted to treat the cases $m = 2g-2$ and $m = n-1$ too. Whereas the method of Xing is fairly simple, to include the above mentioned border cases, we had to overcome several technicalities. It appears that one needs to consider the concept of the decomposition of a code first. A code is called decomposable if it is the direct sum (as codes) of two nonzero codes. Closely related with decomposable codes are codes which stay invariant under the coordinate wise multiplication by an n-tuple of nonzero scalars which are not all the same. In section 2 we show that a geometric Goppa code of length $n > 2g+2$ is not trivial decomposable. Since we need a codeword of weight n in order to get the main result in section 4, we have to extend the field of constants. In section 3 we treat the main properties of divisors and their spaces under an extension of the field of constants. In section 4 we improve Xing's result by showing that if $n > 2g+2$, and G and H have degree m such that $2g-1 < m < n-1$, then G and H define the same code if and only if $G-H$ is the divisor of a rational function which is 1 at the n rational points. If we include the cases $m = 2g-1$ and $m = n-1$, then there are four more possiblities that G and H define the same code. In section 5 the above mentioned characterization of self-dual geometric Goppa codes is given. Section 6 treats some examples to show that we cannot weaken the assumptions we have made. In section 7 we consider the generalized Jacobian and Zeta function to give a formula for the number of linear codes on a curve.

Let $\mathcal{X}$ be a projective, nonsingular, absolutely irreducible curve defined over the finite field $\mathbf{F}_q$. We say that $\mathcal{X}$ is a curve for short. The genus of $\mathcal{X}$ is denoted by $g(\mathcal{X})$ or simply by g when it is clear which curve is meant. Let $\mathbf{F}_q(\mathcal{X})$ be the function field of $\mathcal{X}$ over $\mathbf{F}_q$ and $\Omega_{\mathcal{X}}$ the vector space of rational differential forms on $\mathcal{X}$ over $\mathbf{F}_q$.

Let $P_1, \ldots, P_n$ be n distinct rational points on the curve $\mathcal{X}$. We fix the order of the P_i and denote the divisor $P_1 + \cdots + P_n$ by D . For a rational divisor G on $\mathcal{X}$ with degree m and support disjoint from D we consider the vector spaces
$L(G) = \{f \in \mathbf{F}_q(\mathcal{X})^* \mid (f) \geq -G\} \cup \{0\}$ and $\Omega(G) = \{\omega \in \Omega_{\mathcal{X}} \setminus \{0\} \mid (\omega) \geq G\} \cup \{0\}$.
The algebraic-geometric or geometric Goppa codes asociated to D and G over $\mathbf{F}_q$ are defined by

$$\begin{aligned} C_L(\mathcal{X}, D, G, \mathbf{F}_q) &= \{(f(P_1), ..., f(P_n)) \mid f \in L(G)\}, \\ C_\Omega(\mathcal{X}, D, G, \mathbf{F}_q) &= \{(res_{P_1}(\omega), ..., res_{P_n}(\omega)) \mid \omega \in \Omega(G-D)\}, \end{aligned}$$

see Goppa [5, 6, 7] . We will mainly discuss the codes defined by means of rational functions rather than by differential forms and usually the curve and the field of constants are fixed, therefore we denote $C_L(\mathcal{X}, D, G, \mathbf{F}_q)$ by $C(D, G)$.

For the main properties of geometric Goppa codes we refer to the textbooks on this subject, see [7, 14, 16]. Usually one supposes $\deg(G) < n$ or $\deg(G) > 2g-2$ in order to be able to say something about the dimension and the minimum distance of these codes. That is, if $\deg(G) < n$, then $C_L(D, G)$ has at least dimension $\deg(G) + 1 - g$ and least

minimum distance $n - \deg(G)$. If $\deg(G) > 2g - 2$, then $C_\Omega(D, G)$ has at least dimension $n - \deg(G) - 1 + g$ and at least minimum distance $m - 2g + 2$. If $2g - 2 < \deg(G) < n$, then the dimensions are exactly equal to the above mentioned lower bounds.

2 Decomposable codes

Definition 2.1 If C_1 is an $[n_1, k_1]$ code, and C_2 is an $[n_2, k_2]$ code, then we say that C is the *direct sum* of C_1 and C_2 if (up to reordering of coordinates)

$$C = \{(\mathbf{x}, \mathbf{y}) \mid \mathbf{x} \in C_1, \mathbf{y} \in C_2\}.$$

We denote this by $C = C_1 \oplus C_2$. If moreover C_1 and C_2 are nonzero, then we say that C *decomposes into* C_1 and C_2. We call a linear code C *decomposable* if there exist nonzero codes C_1 and C_2 such that C decomposes into C_1 and C_2.

Remark 2.2 1) The code C decomposes into C_1 and C_2 if and only if (up to reordering of coordinates) C has a generator matrix of the form

$$M = \begin{pmatrix} M_1 & 0 \\ 0 & M_2 \end{pmatrix},$$

where M_1 and M_2 are nonempty generator matrices for C_1 and C_2, respectively.
2) If C decomposes into an $[n_1, k_1, d_1]$ and an $[n_2, k_2, d_2]$ code, then obviously C is an $[n_1+n_2, k_1+k_2, d]$ code, where $d = \min(d_1, d_2)$. Hence $d \leq \frac{n-k}{2}+1$, by the Singleton bound. Thus there are no MDS decomposable codes. Furthermore, if F_1, F_2 and F, respectively, are the weight enumerators of C_1, C_2 and C, respectively, then $F = F_1F_2$.

Example 2.3 Let C be a code of minimum distance one and length greater than one. If $\mathbf{x}$ is a codeword of weight one, then we may assume, after possibly reordering the coordinates, that the first coordinate of $\mathbf{x}$ is not zero. If $\mathbf{x}, \mathbf{y}_1, ..., \mathbf{y}_{k-1}$ is a basis of C, then so is $\mathbf{x}, \mathbf{y}_1 - \lambda_1\mathbf{x}, ..., \mathbf{y}_{k-1} - \lambda_{k-1}\mathbf{x}$, where $\lambda_i = y_{i1}/x_1$. Thus C decomposes in C_1 and C_2, where C_1 is $\mathbf{F}_q$ and C_2 is the projection of C on the last $n-1$ coordinates. We say that codes of minimum distance one and length greater than one are *trivial decomposable.*
The code over $\mathbf{F}_2$ having generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

is decomposable but its dual is not.

Lemma 2.4 *If C is nontrivial decomposable and decomposes into C_1 and C_2, then its dual $C^\perp$ decomposes into $C_1^\perp$ and $C_2^\perp$.*

Proof The inclusion $C_1^\perp \oplus C_2^\perp \subseteq (C_1 \oplus C_2)^\perp$ is obvious. Equality follows by comparing dimensions. If either $C_1^\perp$ or $C_2^\perp$ is zero, then $C_1 = \mathbf{F}_q^{n_1}$ or $C_2 = \mathbf{F}_q^{n_2}$, so C has minimum distance 1, which contradicts the assumption.□

In the following we will discuss decomposable algebraic-geometric codes codes. For that end we need the definition of the intersection of two divisors and Clifford's theorem.

Definition 2.5 Let G be a divisor on a curve $\mathcal{X}$. We denote by $m_P(G)$ the coefficient of G at the place P. So $G = \sum m_P(G)P$. The intersection $G \cap H$ of two divisors G and H on $\mathcal{X}$ is defined as follows

$$G \cap H = \sum \min\{m_P(G), m_P(H)\}P.$$

Lemma 2.6 $L(G) \cap L(H) = L(G \cap H)$

Proof The inclusion $L(G \cap H) \subseteq L(G) \cap L(H)$ follows from the inequalities $G \cap H \leq G$ and $G \cap H \leq H$. Conversely, if $f \in L(G) \cap L(H)$, then

$$v_P(f) \geq \max\{-m_P(G), -m_P(H)\} = -\min\{m_P(G), m_P(H)\} = -m_P(G \cap H),$$

for all places P of $\mathcal{X}$. □

Theorem 2.7 (Clifford) *Let G be a divisor on the curve $\mathcal{X}$ such that both $L(G)$ and $\Omega(G)$ are not zero, then*

$$l(G) \leq \frac{deg(G)}{2} + 1.$$

Moreover equality holds if and only if
a) $\mathcal{X}$ is hyperelliptic and G is a hyperelliptic divisor, or
b) G is a principal divisor, or
c) G is a canonical divisor.

Proof See [16, 2.2.42] or [14, I.6.11].

Corollary 2.8 *Let G be a divisor on a curve $\mathcal{X}$ of genus g such that $0 \leq deg(G) \leq 2g-2$. Then*

$$l(G) \leq \frac{deg(G)}{2} + 1.$$

Moreover equality holds if and only if
a) $\mathcal{X}$ is hyperelliptic and G is a hyperelliptic divisor, or
b) G is a principal divisor, or
c) G is a canonical divisor.

Proof If $l(G) = 0$, then the strict inequality is true. If the index of speciality of G is zero, then by the Riemann-Roch theorem

$$l(G) = \deg(G) + 1 - g < \frac{\deg(G)}{2} + 1.$$

Otherwise the desired result follows from Clifford's Theorem 2.7. □

Proposition 2.9 *Let G be a divisor such that deg$(G) < n$. Then the following statements are equivalent:*
a) $C(D, G)$ is a decomposable code.
b) There are two nonzero effective divisors D_1 and D_2 such that $D_1 + D_2 = D$ and $L(G) = L(G - D_1) \oplus L(G - D_2)$ and both $L(G - D_1)$ and $L(G - D_2)$ are nonzero.
c) There are two nonzero effective divisors D_1 and D_2 such that $D_1 + D_2 = D$ and $L(G) \subseteq L(G - D_1) \oplus L(G - D_2)$ and both $L(G - D_1)$ and $L(G - D_2)$ are nonzero.
d) There are two effective divisors D_1 and D_2 such that $D_1 + D_2 = D$ and $l(G) = l(G - D_1) + l(G - D_2)$ and both $l(G - D_1)$ and $l(G - D_2)$ are nonzero.
If either one of the last three conditions holds, then $C(D, G)$ decomposes into $C(D_1, G-D_2)$ and $C(D_2, G - D_1)$.

Proof We have $L(G - D_1) \cap L(G - D_2) = L((G - D_1) \cap (G - D_2)) = L(G - D) = (0)$, by Lemma 2.6 and since $\deg(G) < n$. Both $L(G - D_1)$ and $L(G - D_2)$ are subspaces of $L(G)$. Hence the last three statements are equivalent. Let us proof the equivalence of (a) and (b). If C is decomposable, then there exist two effective divisors D_1 and D_2 such that $D_1 + D_2 = D$, and a basis $\{f_1, ..., f_s, g_1, ..., g_t\}$ with $(f_i) \geq D_2$ for $i = 1, ..., s$ and $(g_i) \geq D_1$ for $i = 1, ..., t$, so $\{f_1, ..., f_s\} \subseteq L(G - D_2)$ and $\{g_1, ..., g_t\} \subseteq L(G - D_1)$ and (b) is proved. Conversely, if $L(G) = L(G - D_1) \oplus L(G - D_2)$ and $L(G - D_1)$ is generated by $g_1, ..., g_s$ and $L(G - D_2)$ is generated by $f_1, ..., f_t$, then $L(G) =< f_1, ..., f_s, g_1, ..., g_t >$ so $C(D, G)$ decomposes into $C(D_1, G - D_2)$ and $C(D_2, G - D_1)$. □

Corollary 2.10 *If deg$(G) < n$ and $C(D, G)$ is a decomposable code of dimension k, then $k \leq l(2G - D) + 1$.*

Proof For two divisors E_1, E_2 such that $l(E_1)$ and $l(E_2)$ are nonzero, we have

$$l(E_1) + l(E_2) \leq l(E_1 + E_2) + 1,$$

see [16, 2.2.41] or [14, I.6.12]. According to Proposition 2.9 there are two effective divisors D_1 and D_2 such that $D = D_1 + D_2$ and $l(G - D_1) > 0$ and $l(G - D_2) > 0$, so

$$k = l(G - D_1) + l(G - D_2) \leq l(2G - D) + 1.$$

□

Corollary 2.11 *If deg$(G) < n$ and $C(D, G)$ is nontrivial decomposable, then $n \leq 2g + 2$.*

Proof Suppose $C(D, G)$ decomposes into $C(D_1, G)$ and $C(D_2, G)$, with $n_1 = \deg(D_1)$ and $n_2 = \deg(D_2)$. We may assume that $n_1 \leq n_2$. Furthermore $m - n_1 \geq 0$ and $m - n_2 \geq 0$, since $l(G - D_i) \neq 0$ for $i = 1, 2$. Now there are several cases.

Case 1a: If $m - n_1 > 2g - 2$ and $m - n_2 \leq 2g - 2$, then

$$m + 1 - g \leq (m - n_1 + 1 - g) + (\frac{m - n_2}{2} + 1),$$

by Proposition 2.9, the Riemann-Roch Theorem and Corollary 2.8. So $n + n_1 \leq m + 2$. Moreover $m < n$, hence $m = n - 1$ and $n_1 = 1$. Thus the code is trivial decomposable, which is a contradiction.

Case 1b: If $m - n_1 > 2g - 2$ and $m - n_2 > 2g - 2$, then

$$m + 1 - g = (m - n_1 + 1 - g) + (m - n_2 + 1 - g),$$

so $n + g = m + 1$. Moreover $m < n$, hence $m = n - 1$ and $g = 0$. Thus the minimum distance is one, that is the code is trivial decomposable, which is a contradiction.

Case 2: If $m - n_1 \leq 2g - 2$, then $0 \leq m - n_i \leq 2g - 2$ for $i = 1, 2$, since $n_1 \leq n_2$. Thus

$$m + 1 - g \leq (\frac{m - n_1}{2} + 1) + (\frac{m - n_2}{2} + 1),$$

so $n \leq 2g + 2$. $\square$

Example 2.12 Let G be a divisor of degree m on a curve $\mathcal{X}$ of genus g. Suppose $m < n = 2g + 2$. If
a) G has degree $2g + 2$ and there are two nonzero effective divisors D_1 and D_2 such that $D_1 + D_2 = D$ and $G - D_1$ is canonical and $G - D_2$ is principal, or
b) G is not special and $\mathcal{X}$ is hyperelliptic and there are two nonzero effective divisors D_1 and D_2 such that $D_1 + D_2 = D$ and both $G - D_1$ and $G - D_2$ are hyperelliptic divisors,
then $C(D, G)$ is decomposable.
This is a direct consequence of Proposition 2.9.

Proposition 2.13 *Let G be a divisor of degree m on a curve $\mathcal{X}$ of genus g. Suppose $m < n = 2g + 2$. If $C(D, G)$ is nontrivial decomposable, then*
a) G has degree $2g$ and there are two nonzero effective divisors D_1 and D_2 such that $D_1 + D_2 = D$ and $G - D_1$ is canonical and $G - D_2$ is principal, or
b) G is not special and $\mathcal{X}$ is hyperelliptic and there are two nonzero effective divisors D_1 and D_2 such that $D_1 + D_2 = D$ and both $G - D_1$ and $G - D_2$ are hyperelliptic divisors.

Proof We follow the proof of Corollary 2.11. The cases 1a and 1b are similar. In case 2 we now have $0 \leq \deg(G - D_i) \leq 2g - 2$ for $i = 1, 2$. So

$$m + 1 - g = l(G) = (\frac{m - n_1}{2} + 1) + (\frac{m - n_2}{2} + 1),$$

since $n = n_1 + n_2 = 2g + 2$. Thus G is not special and $l(G - D_i) = \deg(G - D_i)/2 + 1$, for $i = 1, 2$.
If $\mathcal{X}$ is not hyperelliptic, then $G - D_i$ is canonical or principal for $i = 1, 2$, by Corollary 2.8. If $G - D_1$ and $G - D_2$ are principal, then the code has dimension 2 and is decomposable, so it is trivial decomposable. If $G - D_1$ and $G - D_2$ are canonical, then $m = 3g - 1$. We assumed $m < n = 2g + 2$, hence $g \leq 2$. But a curve of genus 2 is hyperelliptic. Thus $g = 0, m = 1$ and $n = 2$ or $g = 1, m = 2$ and $n = 4$, in both cases is the code two

dimensional, so trivial decomposable, a contradiction. Therefore one of $G-D_1$ and $G-D_2$ is canonical and the other is principal. Thus $2G-D$ is canonical, so G has degree $2g$.
If $\mathcal{X}$ is hyperelliptic, then $G-D_1$ and $G-D_2$ are hyperelliptic divisors, by Corollary 2.8.
□

Definition 2.14 Let C be a linear code in $\mathbf{F}_q^n$ and σ a permutation of $\{1,\ldots,n\}$. Define

$$\sigma C = \{(x_{\sigma(1)},\ldots,x_{\sigma(n)})|(x_1,\ldots,x_n)\in C\},$$

Two linear codes C_1 and C_2 in $\mathbf{F}_q^n$ are called *equivalent* if $C_2=\sigma C_1$ for some permutation σ of $\{1,\ldots,n\}$. Let $\mathbf{x}$ be an n-tuple of nonzero elements in $\mathbf{F}_q$. Define

$$\mathbf{x}C = \{(x_1c_1,\ldots,x_nc_n)|\mathbf{c}\in C\}.$$

The codes C_1 and C_2 are called *generalized equivalent* or *isometric* if there is an n-tuple $\mathbf{x}$ of nonzero elements in $\mathbf{F}_q$ and a permutation σ such that $C_2=\mathbf{x}\sigma C_1$.

Definition 2.15 We call two divisors G and H *rational equivalent* if there exists a rational function u such that $H=G+(u)$. We will denote this by $G\equiv H$. We call two divisors G and H *rational equivalent with respect to* D if moreover $u(P_i)=1$, for all $i=1,\ldots,n$. We will denote this by $G\equiv_D H$.

Remark 2.16 If $G'=G+(f)$, and the divisors G and G' have disjoint support with D, then $\mathbf{x}C(D,G')=C(D,G)$, where $x_i=f(P_i)$ is not zero. Thus if G and H are rational equivalent and have disjoint support with D, then $C(D,G)$ and $C(D,H)$ are isometric. If G and H are rational equivalent with respect to D, then $C(D,G)=C(D,H)$, see [12, Lemma 3.1].

Proposition 2.17 *Let q be a prime power not equal to 2. If a code C is decomposable, then there exists an n-tuple $\mathbf{x}$ of nonzero elements of $\mathbf{F}_q$, not all the same, such that $\mathbf{x}C=C$. If moreover C is not contained in a coordinate hyperplane, then the converse is also true.*

Proof Suppose C decomposes into C_1 and C_2, where C_i is a nonzero code in $\mathbf{F}_q^{n_i}$, for $i=1,2$. Let $\mathbf{b}$ be the all 1 vector in $\mathbf{F}_q^{n_2}$. Let a an element of $\mathbf{F}_q$ not equal 0 nor 1, and let $\mathbf{a}$ be the all a vector in $\mathbf{F}_q^{n_1}$. Then $\mathbf{a}C_2=C_2$, since C_2 is linear. Let $\mathbf{x}=(\mathbf{a},\mathbf{b})$. Then $\mathbf{x}C=\mathbf{x}(C_1\oplus C_2)=(\mathbf{a}C_1)\oplus(\mathbf{b}C_2)=C_1\oplus C_2$. Thus $\mathbf{x}C=C$.
Conversely, suppose there exists an n-tuple $\mathbf{x}$ of nonzero elements of $\mathbf{F}_q$, not all the same, such that $\mathbf{x}C=C$. Let $\mathbf{x}^i=(x_1^i,\ldots x_n^i)$, then $\mathbf{x}^iC=C$, for all integers i. Suppose that $\mathbf{x}$ has $t+1$ distinct values $a_1,\ldots,a_{t+1}$, then t is at least 1 by assumption. After possibly reordering the coordinates we may assume that the last n_2 coordinates of $\mathbf{x}$ are equal to a_{t+1} and the first n_1 are not, where $n_1+n_2=n$. Let C_1 be the projection of C on $\mathbf{F}_q^{n_1}$ by forgetting the last n_2 coordinates, and let C_2 be the projection of C on $\mathbf{F}_q^{n_2}$ by forgetting the first n_1 coordinates. Both codes C_1 and C_2 are not zero, otherwise C would be contained

in a coordinate hyperplane. Let σ_i be the ith elementary symmetric function in $a_1, \ldots, a_t$, that is

$$\prod_{i=1}^{t}(X - a_i) = \sum_{i=0}^{t}(-1)^i \sigma_i X^{t-i}.$$

Now

$$(\sum_{i=0}^{t}(-1)^i \sigma_i \mathbf{x}^i)C \subseteq C.$$

Suppose $\mathbf{c} \in C$. Let $\mathbf{a}$ consist of the first n_1 coordinates of $\mathbf{c}$ and $\mathbf{b}$ of the last n_2 coordinates, then

$$(\sum_{i=0}^{t}(-1)^i \sigma_i \mathbf{x}^i)\mathbf{c} = \prod_{i=1}^{t}(a_{t+1} - a_i)(0, \ldots, 0, \mathbf{b}).$$

So for all $\mathbf{c} = (\mathbf{a}, \mathbf{b}) \in C$ we have that $(0, \ldots, 0, \mathbf{b}) \in C$, and therefore $(\mathbf{a}, 0, \ldots, 0) \in C$. Thus C is the direct sum of C_1 and C_2. □

Proposition 2.18 *Let G and H be rational equivalent divisors of degree $m < n - 1$ with support disjoint from D on a curve of genus g. Suppose $n = 2g + 2$ and both G and H are special or $n > 2g + 2$. If $C(D, G) = C(D, H)$ and is not contained in a coordinate hyperplane, then G and H are rational equivalent with respect to D.*

Proof The divisors G and H are rational equivalent, hence there exists a rational function u such that $G - H = (u)$. Let $\mathbf{x} = (u(P_1), \ldots, u(P_n))$. Then $\mathbf{x}$ is well defined and an n-tuple of nonzero elements of $\mathbf{F}_q$, since G and H have disjoint support with D. The map $f \mapsto uf$ is an isomorphism from $L(G)$ to $L(H)$, hence $\mathbf{x}C(D, G) = C(D, H)$. We assumed that G and H define the same code, so $\mathbf{x}C(D, G) = C(D, G)$. If all the entries of $\mathbf{x}$ have the same value, then we can divide u by this value, so we may assume that $u(P_i) = 1$ for all i. Thus G and H are rational equivalent with respect to D. If not all the entries of $\mathbf{x}$ are the same, then $C(D, G)$ is decomposable, by Lemma 2.17 since the code is not contained in a coordinate hyperplane, by assumption. The minimum distance of the code is at least $n - m > 1$, by assumption. Hence the code is nontrivial decomposable, so $n \leq 2g + 2$, by Corollary 2.11. So $n = 2g + 2$ and G and H are special, by the assumptions. But this contradicts Proposition 2.13. □

3 Extending the field of constants

In the sequel we need the existence of a codeword of weight n. The existence is often ensured if $q > n$, as the following lemma and its corollary show. Therefore we have to extend the field of constants $\mathbf{F}_q$.

Lemma 3.1 *If C is a linear code in $\mathbf{F}_q^n$ not contained in a coordinate hyperplane, and $n < q$, then there is a codeword in C of weight n.*

Proof Let $C_i = \{\mathbf{c} \in C | c_i = 0\}$. Then $C_i \neq C$ for all i, since C is not contained in a coordinate hyperplane. If there is not a codeword of weight n, then $C \subseteq \cup_{i=1}^{n} C_i$, so, by taking cardinalities we have $q^k \leq nq^{k-1}$, where $k = \dim(C)$. Thus $q \leq n$. This contradicts the assumption $q > n$. □

Corollary 3.2 *If $2g - 1 < deg(G)$ and $n < q$, then there exists in $C(D, G)$ a codeword of weight n.*

Proof If $C(D, G)$ is contained in a coordinate hyperplane $x_i = 0$, then the dual code $C_\Omega(D, G)$ of $C(D, G)$ has a codeword of weight 1. But the minimum distance of $C_\Omega(D, G)$ is at least $\deg(G) - 2g + 2$, which is at least 2, by the assumption on the degree of G. The corollary now follows from Lemma 3.1. □

Definition 3.3 For a given positive integer r let us consider the vector space over $\mathbf{F}_{q^r}$

$$L(G, \mathbf{F}_{q^r}) = \{f \in \mathbf{F}_{q^r}(\mathcal{X})^* \mid (f) \geq -G\} \cup \{0\}.$$

We denote the dimension of $L(G, \mathbf{F}_{q^r})$ over $\mathbf{F}_{q^r}$ by $l(G, \mathbf{F}_{q^r})$. Let the code $C(D, G, \mathbf{F}_{q^r})$ over $\mathbf{F}_{q^r}$ be defined as the image of the map

$$L(G, \mathbf{F}_{q^r}) \longrightarrow \mathbf{F}_{q^r}^n \ ; \ f \mapsto (f(P_1), ..., f(P_n)).$$

Lemma 3.4 *For every divisor G rational over $\mathbf{F}_q$ there exists a basis in $L(G, \mathbf{F}_q)$ for $L(G, \mathbf{F}_{q^r})$ over $\mathbf{F}_{q^r}$. Thus $l(G, \mathbf{F}_q) = l(G, \mathbf{F}_{q^r})$.*

Proof See [16, 2.3.4] or [14, III.6.3.d]. □

Corollary 3.5 *Let G and H be divisors on $\mathcal{X}$, rational over $\mathbf{F}_q$.*
If $C(D, G, \mathbf{F}_q) = C(D, H, \mathbf{F}_q)$, then $C(D, G, \mathbf{F}_{q^r}) = C(D, H, \mathbf{F}_{q^r})$.

Proof This follows directly from Lemma 3.4. □

Lemma 3.6 *If G and H are two divisors defined over $\mathbf{F}_q$ and rational equivalent (with respect to D) over $\mathbf{F}_{q^r}$, then they are rational equivalent (with respect to D) over $\mathbf{F}_q$ itself.*

Proof See [14, III.6.3.f]. □

4 Equality of codes and rational equivalence of divisors with respect to D

In this section we determine conditions which imply that the divisors G and H are equal or rational equivalent with respect to D whenever they define the same code. For the main idea we will follow Xing [17]. In his work he assumes that G and H have the same degree m and $2g - 1 < m < n - 1$, for the main result he assumes $m < n/2$ or $m > n/2 + 2g - 2$.

His results are based on Clifford's theorem. We will improve his results by admitting also the values $2g-1$ and $n-1$ for m, and assuming $n > 2g+2$ only.

Definition 4.1 Let $P_1, \ldots, P_n$ be n distinct rational points on a curve $\mathcal{X}$. Fix a differential η on a the curve $\mathcal{X}$ such that η has simple poles and residue 1 at these rational points. Such a differential exists, see [11, Corollary 2.6]. Let W be the divisor of η. Define for every divisor G on $\mathcal{X}$, the divisor $G^\perp$ by $G^\perp = D + W - G$.

Remark 4.2 If G is a divisor with disjoint support with D and degree smaller than n, or greater than $2g-2$, respectively, then $G^\perp$ is a divisor with disjoint support with D and degree greater than $2g-2$, or smaller than n, respectively. Furthermore $C(D, G^\perp) = C(D, G)^\perp = C_\Omega(D, G)$, see [11].

Example 4.3 Let $\mathcal{X}$ be a curve of genus $g > 0$ and at least $n > 2g+2$ rational points. Let $P_1, \ldots, P_n$ be n distinct rational points on $\mathcal{X}$, and define $D = P_1 + \cdots + P_n$. Let K and W be canonical divisors on the curve $\mathcal{X}$, with disjoint support with D. Let P and Q be two different rational points of $\mathcal{X}$, not in the support of D. Let $G = K + P$ and $H = W + Q$. Then $L(G)$ and $L(K)$ have dimension g, and $L(G)$ contains $L(K)$, so these two vector spaces are the same and in the same way we have $L(H) = L(W)$. If K and W are equivalent with respect to D, then they define the same code, thus G and H have degree $2g-1$ and define the same code but are not equivalent. In other words if $G-P$ and $H-Q$ are equivalent with respect to D and are canonical divisors, then G and H define the same code. Dualy $G^\perp$ and $H^\perp$ are two divisors of the same degree $n-1$ and define the same code. In other words if $G'+P$ and $H'+Q$ are equivalent with respect to D and are equivalent with D, then G' and H' define the same code.
There is another way that two divisors of degree $2g-1$ or n, respectively, define the same code. If $G-P_i$ and $H-P_i$ are equivalent with respect to $D-P_i$ and are canonical divisors, then G and H define the same code. This is seen in the same way as above. Dually, if $G+P_i$ and $H+P_i$ are equivalent with respect to $D-P_i$ and are equivalent with D, then G and H define the same code. This explains why Xing [17] assumes $2g-1 < \deg(G) < n-1$.

Remark 4.4 The following properties follow immediately from the definitions.
Let G and H be two divisors on $\mathcal{X}$. Then
a) If G and H have the same degree, then $G \neq H$ if and only if $\deg(G \cap H) < \deg(G)$.
b) $G^\perp \cap H^\perp = D + W - G - H + G \cap H$.
c) $G + H - G \cap H - D$ is canonical if and only if $G^\perp \cap H^\perp$ is principal.
d) $G^\perp + H^\perp - G^\perp \cap H^\perp - D$ is canonical if and only if $G \cap H$ is principal.

Proposition 4.5 *Let E and F be two divisors on a curve of genus g. Suppose $l(F)$ is not zero and $2g-1 \leq deg(F)$. If $deg(E) < deg(F)$, then $l(E) < l(F)$ or E is canonical and $deg(F) = 2g-1$. Moreover if $E \leq F$, $E \neq F$ and $l(E) = l(F)$, then E is canonical and there is a rational point P such that $F = E + P$.*

Proof If $\deg(E) < 0$, then $l(E) = 0 < l(F)$. So we may assume that $\deg(E) \geq 0$. The inequality follows directly from the Riemann-Roch Theorem, by distinguishing between the two cases: $\deg(E) > 2g-2$ and $0 \leq \deg(E) \leq 2g-2$. In the first case we have $l(E) < l(F)$. In the second case we have $l(E) \leq g \leq l(F)$, by Corollry 2.8 and since $\deg(F) \geq 2g-1$. If $l(E) = l(F)$, then $g \leq l(F) = l(E) \leq \deg(E)/2 + 1 \leq g$, by Corollary 2.8. Thus l(E)=deg(E)/2 +1=g, so E is canonical, by Corollary 2.8. So $\deg(F) = 2g-1$. If moreover $E \leq F$, then $F = E + P$, for some effective divisor P. Comparing the degrees of E and F implies P has degree one. Thus P is a rational point. □

Corollary 4.6 *If G and H are two divisors of the same degree m on a curve of genus g such that $m > 2g-2$ and $l(G) > 0$, then $L(G) = L(H)$ if and only if $G = H$ or $G \cap H$ is canonical and $G = G \cap H + P$ and $H = G \cap H + Q$ for some rational points P and Q.*

Proof This is a direct consequence of Proposition 2.6 applied to the divisors $E = G \cap H$ and $F = G$ or $F = H$. □

Proposition 4.7 *Let G and H be two divisors of the same degree m on a curve of genus g. If $2g-2 < m < n$ and $C(D,G) = C(D,H)$, then*

$$l(G) \leq l(G \cap H) + l(G + H - G \cap H - D).$$

Proof We follow Xing [17]. For every $f \in L(G)$ there exists a unique element $h_f \in L(H)$ defining the same codeword, since $C(D,G) = C(H,D)$ and $\deg(G) = \deg(H) < n$. Consider the $\mathbf{F}_q$ linear map

$$\phi : L(G) \longrightarrow \mathbf{F}_q(\mathcal{X}); \quad \phi(f) = f - h_f.$$

Let V be the image of the map ϕ. Then $\mathrm{Ker}(\phi) = L(G \cap H)$, by Proposition 2.6. Thus V is isomorphic to $L(G)/L(G \cap H)$, so $l(G) = l(G \cap H) + \dim(V)$. Remark that if $f \in L(G)$ and $h \in L(H)$, then $f - h \in L(G + H - G \cap H)$, since

$$\begin{aligned} v_P(f-h) &\geq \min\{v_P(f), v_P(h)\} \\ &\geq \min\{-m_P(G), -m_P(H)\} \\ &= -m_P(G) - m_P(H) + \min\{m_P(G), m_P(H)\} \\ &= -m_P(G) - m_P(H) + m_P(G \cap H), \end{aligned}$$

for all places P of $\mathcal{X}$. If moreover $h = h_f$, then $(f - h_f)(P_i) = 0$, for all $i = 1, \ldots, n$, since f and h_f define the same codeword. Thus $V \subseteq L(G + H - G \cap H - D)$, and we conclude $l(G) \leq l(G \cap H) + l(G + H - G \cap H - D)$. □

Proposition 4.8 *Let G and H be two divisors of the same degree m on a curve of genus g. If $C(D,G)$ is not zero, $2g-2 < m < n$ and deg$(G \cap H) > 2m - n$, then $C(D,G) = C(D,H)$ if and only if*
a) $G = H$, or
b) there exist two rational points P and Q such that $G - P = H - Q$ and is a canonical divisor.

Proof If a) $G = H$, or b) there exist two rational points P and Q such that $G-P = H-Q$ is a canonical divisor, then G and H define the same code, as we have seen in Example 4.3. Conversely, suppose $C(D,G) = C(D,H)$. If $G \neq H$, then $\deg(G \cap H) < \deg(G)$, by Remark 4.4. So $G \cap H$ is a canonical divisor and $G = G \cap H + P$ for some rational point P or $l(G \cap H) < l(G)$, by Lemma 4.5. In the first case we also have $H = G \cap H + Q$ for some rational point Q, thus $G - P = H - Q$ is a canonical divisor. In the second case we get $l(G \cap H) < l(G) \leq l(G \cap H)$, by Proposition 4.7, since $l(G + H - G \cap H - D) = 0$, by the assumption $\deg(G \cap H) > 2m - n$. This gives a contradiction. Therefore $G = H$. □

Proposition 4.9 *Let G and H be two divisors of the same degree m on a curve of genus g. If $C(D,G)$ is not equal to $\mathbf{F}_q^n$, $2g-2 < m < n$ and deg$(G \cap H) > 2g-2$, then $C(D,G) = C(D,H)$ if and only if*
a) $G = H$, or
b) there exist two rational points P and Q such that $G+P = H+Q$ and is equivalent with D.

Proof By Remark 4.4, we have,

$$G^{\perp} \cap H^{\perp} = D + W - G - H + G \cap H = G^{\perp} + H^{\perp} - D - W + G \cap H.$$

So if $\deg(G \cap H) > 2g-2$, then $\deg(G^{\perp} \cap H^{\perp}) > 2\deg(G^{\perp}) - n$. If $l(G) \neq n$, then $l(G^{\perp}) \neq 0$. Therefore the assertion we want to proof follows from Proposition 4.8 by duality. □

Lemma 4.10 *Let G and H be two divisors of the same degree m on a curve of genus g such that $2g-2 < m < n$. Suppose $0 \leq$ deg$(G \cap H) \leq 2g-2$ and $0 \leq$ deg$(G+H-G \cap H-D) \leq 2g-2$. If $C(D,G) = C(D,H)$, then $n \leq 2g+2$.*

Proof Proposition 4.7 gives

$$m + 1 - g \leq (\frac{\deg(G \cap H)}{2} + 1) + (\frac{\deg(G + H - G \cap H - D)}{2} + 1) = m - \frac{n}{2} + 2.$$

Thus $n \leq 2g + 2$. □

Remark 4.11 If G and H are rational equivalent with respect to D, then

$$G = H \quad \text{or} \quad \deg(G \cap H) \leq m - n.$$

This is seen as follows. By assumption we have $H = G + (u)$, where u is a rational function such that $u(P_i) = 1$, for all $i = 1, \ldots, n$. Suppose $G \neq H$. Then $u \neq 1$, so $u - 1$ is not zero. So $(u-1)(P_i) = 0$, for all $i = 1, \ldots, n$, and $(u-1) \geq D - (u)_{\infty}$. Therefore $\deg(u)_{\infty} = \deg((u-1)_0) \geq \deg(D) = n$. Furthermore $G \cap H = G \cap (G + (u)_0 - (u)_{\infty}) = G - (u)_{\infty}$. Thus $\deg(G \cap H) \leq \deg(G) - n$. This explains the condition $\deg(G \cap H) > m - n$ in the next theorem.

Theorem 4.12 *Suppose $n > 2g+2$. Let G and H be two divisors of the same degree m on a curve of genus g. If $C(D,G)$ is not equal to 0 nor to $\mathbf{F}_q^n$, $2g-2 < m < n$ and deg$(G \cap H) > m-n$, then $C(D,G) = C(D,H)$ if and only if*
a) $G = H$, or
b) there exist two rational points P and Q such that $G-P$ and $H-Q$ are equivalent with respect to D and are canonical divisors, or
c) there exist two rational points P and Q such that $G+P$ and $H+Q$ are equivalent with respect to D and are equivalent with D, or
d) there exists an i, $0 \leq i \leq n$, such that $G-P_i$ and $H-P_i$ are equivalent with respect to $D-P_i$ and are canonical divisors, or
e) there exists an i, $0 \leq i \leq n$, such that $G+P_i$ and $H+P_i$ are equivalent with respect to $D-P_i$ and are equivalent with D.

Proof We have to proof only one direction of the theorem by Example 4.3.

1) If $\deg(G \cap H) > 2g-2$, then $G = H$ or there exist two rational points P and Q such that $G+P = H+Q$ are equivalent with D, by Proposition 4.9; thus we are in case (a) or (c). So we may assume that $\deg(G \cap H) \leq 2g-2$. If $\deg(G^\perp \cap H^\perp) > 2g-2$, then $G = H$ or there exist two rational points P and Q such that $G-P = H-Q$ are canonical divisors, by duality; thus we are in case (a) or (b). So we may assume $\deg(G^\perp \cap H^\perp) \leq 2g-2$, hence $\deg(G+H-G \cap H-D) \geq 0$, by Remark 4.4.

2) If $\deg(G \cap H) < 0$, then $l(G \cap H) = 0$, thus $l(G) \leq l(G+H-G \cap H-D)$, by Proposition 4.7. The assumption $\deg(G \cap H) > m-n$, implies $\deg(G+H-G \cap H-D) < \deg(G)$. We already have $\deg(G+H-G \cap H-D) \geq 0$, by (1). Thus $\deg(G) = 2g-1$ and $G+H-G \cap H-D$ is a canonical divisor, by Proposition 4.5.

2a) If the code $C(D,G)$ is contained in a coordinate hyperplane, of say the ith coordinate, then P_i is a base point of G and H. Let $E_i = E - P_i$ for a divisor E. Thus G_i and H_i are canonical divisors, have disjoint support with D_i and $C(G_i, D_i) = C(H_i, D_i)$. The divisors G_i and H_i are base point free, so the code $C(G_i, D_i)$ is not contained in a coordinate hyperplane. Moreover D_i has degree $n-1 \geq 2g+2 > 2g-2 = \deg(G_i)$. The divisors G_i and H_i are equivalent and special. Thus G_i and H_i are equivalent with respect to D_i, by Proposition 2.18, thus we are in case (d).

2b) If $C(D,G)$ is not contained in a coordinate hyperplane, then, after possibly extending the field of constants say from $\mathbf{F}_q$ to $\mathbf{F}_{q^r}$, there exists a code word $\mathbf{c}$ of weight n, by Lemma 3.1. Let f and h be the rational functions in $L(G)$ and $L(H)$, respectively, giving the word $\mathbf{c}$. Let $u = f/h$ then $u(P_i) = 1$, since $f(P_i) = h(P_i) = c_i$ is not equal to zero. Now $h = f/u$, thus h is a nonzero element of $L(H)$ and $L(G+(u))$, so $L(H \cap (G+(u))$ is not zero, therefore deg $(H \cap (G+(u)) \geq 0$. Let $G' = G+(u)$, then G and G' define the same code, by Remark 2.16, and $\deg(H \cap G') \geq 0 > m-n$. If $H = G'$, then G and H are equivalent with respect to D, and $\deg(G \cap H) > m-n$, so $G = H$, by Remark 4.11, thus we are in case (a). So we may assume that $H \neq G'$. Now we follow (1) again. If $\deg(H \cap G') > 2g-2$, then there exist two $\mathbf{F}_{q^r}$-rational points P and Q such that $G'+P = H+Q$ and is equivalent with D, since $H \neq G'$. But $H+Q$ has degree $2g$ and D has degree $n > 2g+2$, so this is impossible. Thus $0 \leq \deg(H \cap G') \leq 2g-2$.

If $\deg(G'^{\perp} \cap H^{\perp}) > 2g-2$, then there exist two $\mathbf{F}_{q^r}$-rational points P and Q such that $G' - P = H - Q$ are canonical divisors, by duality and since $H \neq G'$. So $G - P$ and $H - Q$ are equivalent with respect to D, and canonical. Now we show that P and Q are $\mathbf{F}_q$ rational. Let K be a $\mathbf{F}_q$ rational canonical divisor, such a divisor exists, then $G - K$ is $\mathbf{F}_q$ rational and equivalent with P, thus $l(G-K, \mathbf{F}_{q^r}) = l(P, \mathbf{F}_{q^r}) > 0$. So $l(G-K, \mathbf{F}_q) > 0$, by Lemma 3.4, so there exists a nonzero $\mathbf{F}_q$-rational function v such that $(v) \geq -G + K$, so $(v) - G + K$ is an effective $\mathbf{F}_q$-rational divisor of degree 1, that is a $\mathbf{F}_q$-rational point P'. Moreover P and P' are equivalent over $\mathbf{F}_{q^r}$, and the genus is not zero, since G has degree $2g-1$ and $l(G) > 0$, thus $P = P'$ is a $\mathbf{F}_q$-rational point. In the same way it is proved that Q is an $\mathbf{F}_q$-rational point. Therefore there exist two $\mathbf{F}_q$-rational points P and Q such that $G + P$ and $H + Q$ are equivalent with respect to D and canonical; this is case (b).
Therefore we may assume $\deg(G'^{\perp} \cap H^{\perp}) \leq 2g-2$, so $\deg(G' + H - G' \cap H - D) \geq 0$. Now $0 \leq \deg(G' + H - G' \cap H - D) \leq \deg(G' + H - D) = 2(2g-1) - n \leq 2g-2$, since $n > 2g+2$. Thus $n \leq 2g+2$, by Lemma 4.10 which gives a contradiction.

3) From (1) and (2) we conclude that we may assume $0 \leq \deg(G \cap H) \leq 2g-2$. By duality we have cases (a), (b), (c) or (e) or we may assume $0 \leq \deg(G^{\perp} \cap H^{\perp}) \leq 2g-2$, hence $0 \leq \deg(G + H - G \cap H - D) \leq 2g-2$. Thus $n \leq 2g+2$, by Lemma 4.10, which is a contradiction. □

Corollary 4.13 *Suppose $n > 2g+2$. Let G and H be two effective divisors of the same degree m on a curve of genus g. If $C(D,G)$ is not equal to 0 nor to $\mathbf{F}_q^n$ and $2g-2 < m < n$, then $C(D,G) = C(D,H)$ if and only if*
a) $G = H$, or
b) there exist two rational points P and Q such that $G - P$ and $H - Q$ are equivalent with respect to D and are canonical divisors, or
c) there exist two rational points P and Q such that $G + P$ and $H + Q$ are equivalent with respect to D and are equivalent with D, or
d) there exists an i, $0 \leq i \leq n$, such that $G - P_i$ and $H - P_i$ are equivalent with respect to $D - P_i$ and are canonical divisors, or
e) there exists an i, $0 \leq i \leq n$, such that $G + P_i$ and $H + P_i$ are equivalent with respect to $D - P_i$ and are equivalent with D.

Proof This follows from Theorem 4.12, since $m - n < 0 \leq \deg(G \cap H)$. □

Theorem 4.14 *Suppose $n > 2g+2$. Let G and H be two divisors of the same degree m on a curve of genus g. If $C(D,G)$ is not equal to 0 nor to $\mathbf{F}_q^n$ and $2g-2 < m < n$, then $C(D,G) = C(D,H)$ if and only if*
a) G and H are equivalent with respect to D, or
b) there exist two rational points P and Q such that $G - P$ and $H - Q$ are equivalent with respect to D and are canonical divisors, or
c) there exist two rational points P and Q such that $G + P$ and $H + Q$ are equivalent with respect to D and are equivalent with D, or
d) there exists an i, $0 \leq i \leq n$, such that $G - P_i$ and $H - P_i$ are equivalent with respect to

$D - P_i$ and are canonical divisors, or
e) there exists an i, $0 \leq i \leq n$, such that $G + P_i$ and $H + P_i$ are equivalent with respect to $D - P_i$ and are equivalent with D.

Proof: After Example 4.3 we have to prove only one direction of the assertion.
If the code $C(D, G)$ is contained in a coordinate hyperplane, then we proceed according to (2a) of the proof of Theorem 4.12. If $C(D, G)$ is not contained in a coordinate hyperplane, then, after possibly extending the field of constants, there exists a code word $\mathbf{c}$ of weight n, by Lemma 3.1. Let f and h be the rational functions in $L(G)$ and $L(H)$, respectively, giving the word $\mathbf{c}$. Consider the divisors $G' = G + (f), H' = H + (h)$. It is clear that G' and H' are effective divisors with support disjoint with D. Furthermore,

$$C(D, G) = (f(P_1), ..., f(P_n))C(D, G') = \mathbf{c}C(D, G'),$$

and similarly $C(D, H) = \mathbf{c}C(D, H')$, as we have seen in Remark 2.16, so $\mathbf{c}C(D, G') = \mathbf{c}C(D, H')$. Thus $C(D, G') = C(D, H')$, since $\mathbf{c}$ has nonzero entries. The theorem now follows from Corollary 4.13 and the fact that if $G' = H'$, then G and H are equivalent with respect to D. The equivalence (with respect to D), is possibly defined over a finite extension of $\mathbf{F}_q$, but then it is also equivalent over $\mathbf{F}_q$, by Lemma 3.6. □

Corollary 4.15 *Suppose $n > 2g + 2$. Let G and H be two divisors of the same degree m on a curve of genus g. If $C(D, G)$ is not equal to 0 nor to $\mathbf{F}_q^n$ and $2g - 1 < m < n - 1$, then $C(D, G) = C(D, H)$ if and only if G and H are equivalent with respect to D.*

Proof This is a direct consequence of Theorem 4.14, since in the cases (b),(c)(d) and (e) we have either $m = 2g - 1$ or $m = n - 1$. □

5 Self-dual codes

In this section we obtain a neccesary and sufficient condition for self-duality of a geometric Goppa code $C(D, G)$ in terms of G and D. The question on self-dual codes was considered before by Driencourt, Michon, Stichtenoth and Xing, see [1, 2, 3, 4, 11, 12, 17]. The best result so far is if $n > 6g - 4$, then G defines a self-dual code if and only if there exists a differential form η such that $(\eta) = 2G - D$ and η has residue 1 at all points of D, see [17, Corollary 4]. We will show that the assumption $n > 2g + 2$ instead of $n > 6g - 4$ is sufficient for the characterization to hold. In the next section we generalize an example of [4] which shows that the characterization fails in case $n = 2g + 2$.

Definition 5.1 A code C is *self-dual* if it coincides with its dual $C^\perp$. In the same way, a code C is called *formal self-dual* if there exists an n-tuple $\mathbf{x}$ of nonzero elements in $\mathbf{F}_q$ such that $C^\perp = \mathbf{x}C$; thus C is formal self-dual if and only if it is self-dual with respect to the bilinear form

$$< \mathbf{a}, \mathbf{b} >= \sum x_i a_i b_i.$$

Remark 5.2 We already remarked in 4.1 that for a given curve $\mathcal{X}$ and $D = P_1 + \cdots + P_n$ there exists a differential form ω on $\mathcal{X}$ with simple poles and residue 1 at every P_i such that for every divisor G we have that $C(D,G)^\perp = C(D, D + W - G)$, where W is the divisor of ω. Thus we immediately get the following sufficient condition for (formal) self-duality.

Proposition 5.3 *If there exists a differential form η with simple poles at every P_i such that $2G = D + K$, where $K = (\eta)$, then $C(D,G)$ is formal self-dual. If moreover $res_{P_i}(\eta) = 1$ for all P_i, then $C(D,G)$ is self-dual.*

Proof See [11]. □

Remark 5.4 If there exists a divisor G such that $2G = D + K$, where K is a canonical divisor, then $D \equiv 2A$ for some divisor A, see [9] or [16, 3.1.3].

Theorem 5.5 *Assume $n > 2g + 2$.*
a) The code $C(D,G)$ is self-dual if and only if there exists a differential form η with simple poles and residue 1 at every P_i such that $2G = D + K$, where $K = (\eta)$.
b) The code $C(D,G)$ is formal self-dual if and only if there exists a differential form η with simple poles at every P_i such that $2G = D + K$, where $K = (\eta)$.

Proof One direction of the theorem is Proposition 5.3. Now we prove the converse. Let k be the dimension of the code $C(D,G)$. Then $k = l(G) - l(G - D)$. If $\deg(G) \leq 2g - 2$ then $k \leq g$, by Clifford's theorem. Hence, if $\deg(G) \geq n$, then $k \geq n - g$, by duality. Taking into account that $k = n/2$ whenever $C(D,G)$ is (formal) self-dual and the assumption $n > 2g + 2$, we get $2g - 1 < \deg(G) < n - 1$. Now $C(D,G)^\perp = C(D,G^\perp)$ and $G^\perp = W + D - G$, where W is the divisor of a differential with simple poles and residue 1 at every P_i. Suppose $C(D,G)$ is self-dual. Then G and $G^\perp$ have the same degree m such that $2g - 1 < m < n - 1$ and define the same code, so there is a rational function f such that $2G = D + W + (f)$ and f is 1 at all P_i, by Corollary 4.15. Now it suffices to take $\eta = f\omega$. If $C(D,G)$ is formal self-dual, that is there exists an n-tuple $\mathbf{x}$ of nonzero elements in $\mathbf{F}_q$ such that $C(D,G)^\perp = \mathbf{x}C(D,G)$, then we can find a rational function h such that $h(P_i) = x_i$, by the independance of valuations. Thus $\mathbf{x}C(D, G^\perp + (h)) = C(D,G^\perp)$, by Remark 2.16. So $C(D, G^\perp + (h)) = C(D,G)$ and we can proceed as above. □

In case $n \leq 2g + 2$ the conclusion of the theorem is not true as we shall see in the examples of the next section.

6 Examples

Example 6.1 This example is a generalization of the one given by Driencourt and Stichtenoth [4], where $q = 4$. Let q be an even power of 2. Let $\mathcal{X}$ be the curve defined over $\mathbf{F}_q$ with the following affine equation

$$Y^2 + Y = X^{q-1}.$$

So this curve has function field $\mathbf{F}_q(x,y)$, where $y^2+y=x^{q-1}$. The curve $\mathcal{X}$ is hyperelliptic and has genus $\frac{1}{2}q-1$. Let α be a solution in $\mathbf{F}_q$ of the equation X^2+X+1, it exists since q is an even power of 2. Let β be a primitive element of $\mathbf{F}_q$. Define $\alpha_1=0$ and $\alpha_i=\beta^i$ for $2\leq i\leq q$. Let $P_1=(0,0)$ and $Q_1=(0,1)$. Let $P_i=(\alpha_i,\alpha)$ and $Q_i=(\alpha_i,\alpha^2)$ for $2\leq i\leq q$. Let P_∞ be the unique point at infinity of $\mathcal{X}$. The curve has exactly $2q+1$ rational points, that is

$$\mathcal{X}(\mathbf{F}_q)=\{P_i,Q_i|1\leq i\leq q\}\cup\{P_\infty\}$$

The point P_∞ is a hyperelliptic Weierstrass point. Take $G=(q-2)P_\infty$. Then $L(G)$ has as a basis

$$1,x,\ldots,x^{\frac{1}{2}q-1}.$$

Let $D=P_1+\cdots+P_q$. Let C be the code $C=C(\mathcal{X},D,G)$. Then C is a Reed-Solomon code, that is a code on the projective line $\mathbf{P}^1$. Since, if we take $R_i=(\alpha_i:1)$, $R_\infty=(1:0)$, $D'=R_1+\cdots+R_q$ and $G'=(\frac{1}{2}q-1)R_\infty$, then $C=C(\mathbf{P}^1,D',G')$. Now $2G'-D'=(q-2)R_\infty-(R_1+\cdots+R_q)$, which is the divisor of the differential η on $\mathbf{P}^1$, where

$$\eta=\left(\prod_{i=1}^{q}(x-\alpha_i)\right)^{-1}dx.$$

Furthermore η has simple poles and residue 1 at R_i for $1\leq i\leq q$. Thus C is self-dual, by Proposition 5.3. Thus we have a self-dual code $C(D,G)$ on $\mathcal{X}$, and $g=\frac{1}{2}q-1$, $\deg(G)=q-2=2g$ and $n=q=2g+2$. We claim that $2G-D$ is not a canonical divisor. The divisor $(q-4)P_\infty$ is canonical, since it is the divisor of dx. If $2G-D$ is canonical, then $(2q-4)P_\infty-(P_1+\cdots+P_q)$ is equivalent with $(q-4)P_\infty$. So qP_∞ is equivalent with $P_1+\cdots+P_q$. Therefore there exists a nonzero rational function f on $\mathcal{X}$ such that $(f)=P_1+\cdots+P_q-qP_\infty$. So f is a nonzero element of the vector space $L(qP_\infty)$, which has basis

$$1,x,\ldots,x^{\frac{1}{2}q-1},y,x^{\frac{1}{2}q}.$$

Thus

$$f=\sum_{i=0}^{\frac{1}{2}q}a_ix^i+by.$$

Let

$$F=\sum_{i=0}^{\frac{1}{2}q}a_iX^i+b\alpha.$$

Then $F(\alpha_i)=f(P_i)=0$ for $2\leq i\leq q$. Thus F is a polynomial of degree $\frac{1}{2}q$ and has at least $q-1$ zeros, and therefore $F=0$, since $q\geq 4$. So $f=-b\alpha+by$, but $0=f(P_1)=-b\alpha$ and $\alpha\neq 0$. Thus $b=0$, so $f=0$, which is a contradiction. Therefore $2G-D$ is not canonical.

If we consider the differential η but now viewed on $\mathcal{X}$, then

$$(\eta)=(3q-4)P_\infty-(P_1+\cdots+P_q+Q_1+\cdots+Q_q).$$

This differential has simple poles and residue 1 at all points P_i. Now

$$G^\perp = D + (\eta) - G = (2q-2)P_\infty - (Q_1 + \cdots + Q_q).$$

The code $C(D,G)$ is self-dual, so $C(D,G) = C(D,G^\perp)$, and G and $G^\perp$ are not equivalent. Consider the rational function $h = \alpha(y-1)(y-\alpha^2)$. It has divisor

$$(h) = (q-1)Q_1 + Q_2 + \cdots + Q_q - (2q-2)P_\infty.$$

Furthermore $h(P_i) = 1$ for $1 \leq i \leq q$. Let $H = (q-2)Q_1$, then $H = G^\perp + (h)$. Thus H and G are two divisors of degree $2g$ which define the same code of length $2g+2$, which are not equivalent, and $G \cap H = 0$ and $G + H - G \cap H - D$ is canonical.

Remark 6.2 If one looks at the proof of case 3 of Theorem 4.12 in case $n = 2g+2$ and $\mathcal{X}$ is not (hyper)elliptic, then $G \cap H$ and $G + H - G \cap H - D$ are principal or canonical divisors. If they are at the same time principal, then $2m = n = 2g+2$, so $m = g+1$, this contradicts the assumptions $m > 2g-2$ and $\mathcal{X}$ is not (hyper)elliptic. In the same way we get a contradiction with the assumtions in case $G \cap H$ and $G + H - G \cap H - D$ are canonical. An example of the case that the first one is canonical and the second is principal can be constructed as follows. Let K be a canonical divisor and let $G = K + A$ and $H = K + B$, where A and B are effective divisors of degree 2 with disjoint support and which are not equivalent. The vector spaces $L(G)$ and $L(H)$ both have dimension $g+1$ and have as intersection the space $L(K)$ of dimension g. Let f be an element of $L(G) \setminus L(K)$ and h an element of $L(H) \setminus L(K)$. So $(f-h) \geq -G - H + K$ and $(f-h) + G + H - K$ is an effective divisor of degree $2g+2$. If we could choose f and h in such a way that $f-h$ is zero at $2g+2$ rational points not in the support of G nor of H, then we can take for D the sum of these $2g+2$ rational points and thus the codes $C(D,G)$ and $C(D,H)$ are the same, whereas the divisors G and H are not equivalent. In the following we give an explicit example.

Example 6.3 Let r be an odd power of 3, and $q = r^2$. Consider the Hermitian projective plane curve $\mathcal{X}$ over $\mathbf{F}_q$ with affine equation $X^{r+1} = Y^r + Y$, see [13, 15]. It has genus $g = r(r-1)/2$ and r^3+1 rational points. The function field of $\mathcal{X}$ is $\mathbf{F}_q(x,y)$, where $x^{r+1} = y^r + y$. Let β be an element of $\mathbf{F}_q$ such that $\beta^r + \beta = 1$, such an element exists since the trace from $\mathbf{F}_q$ to $\mathbf{F}_r$ is surjective. Let α be a primitive element of $\mathbf{F}_q$ and $\alpha_i = \alpha^{i(r-1)}$, then the α_i for $0 \leq i \leq r$ are the $r+1$ distinct solutions of the equation $X^{r+1} = 1$. So there lie $r+1$ distinct rational points on the intersection of the curve $\mathcal{X}$ and the line with equation $Y = \beta$. In fact every line in the projective plane, defined over $\mathbf{F}_q$, intersects the curve $\mathcal{X}$ in exactly $r+1$ rational points or is tangent at a rational point of this curve with multiplicity $r+1$. Let $Q_{r-2} = (1,\beta)$, $Q_{r-1} = (-1,\beta)$, $Q_r = (\gamma,\beta)$ and $Q_{r+1} = (-\gamma,\beta)$, where $\gamma^2 = -1$, then these four points lie on the intersection of the curve with the line with equation $Y = \beta$, and let $Q_1, \cdots, Q_{r-3}$ be the remaining $r-3$ rational points on this intersection. Let P_∞ be the unique rational point at infinity. Define the divisors G and H as follows,

$$G = (r^2-1)P_\infty - (Q_1 + \cdots + Q_{r-1}) \quad \text{and}$$

$$H = (r^2-1)P_\infty - (Q_1 + \cdots + Q_{r-3} + Q_r + Q_{r+1}).$$

Then $K = G \cap H = (r^2-1)P_\infty - (Q_1 + \cdots + Q_{r+1})$ is a canonical divisor, and $G = K + A$ and $H = K + B$, where $A = Q_r + Q_{r+1}$ and $B = Q_{r-2} + Q_{r-1}$. The vector space $L(K)$ has basis $\{x^i y^j (y-\beta) | 0 \leq i + j \leq r-2\}$. Let $a(X) = (X^{r+1}-1)/(X^4-1)$. The polynomial $X^{r+1}-1$ is divisible by X^4-1, since r is an odd power of 3. So $a(X)$ is a polynomial. Now $L(G) = L(K) + < (x^2-1)a(x) >$ and $L(H) = L(K) + < (x^2+1)a(x) >$. Let $f = -a(x)y(y-\beta) - \beta^r a(x)(x^2-1)$ and let $h = a(x)y(y-\beta) - \beta^r a(x)(x^2+1)$. Then f is an element of $L(G) \backslash L(K)$, and h is an element of $L(H) \backslash L(K)$. Now $f - h = a(x)(y-1)(y+\beta^r)$ and is an element of $L(G+H-K)$. The function $f-h$ is zero at r^2-1 distinct rational points. Among the zeros are the points $Q_1 + \cdots + Q_{r-3}$, the remaining $r^2 - r + 2$ points we denote by $P_1, \ldots, P_n$, where $n = r^2 - r + 2 = 2g + 2$. Thus the divisor of $f - h$ is equal to

$$Q_1 + \cdots + Q_{r-3} + P_1 + \cdots + P_n - (r^2-1)P_\infty = -G - H + G \cap H + D.$$

Therefore the codes $C(D, G)$ and $C(D, H)$ are the same, but the divisors G and H are not equivalent.

7 Generalized Jacobian and Zeta function

In this section we study the question how many geometric codes there are arising from D, where we leave the order of the P_i's fixed.

Definition 7.1 Let $\mathrm{Div}(\mathcal{X}, D)$ be the abelian group of divisors on $\mathcal{X}$ with disjoint support with D, and let $\mathrm{Div}_m(\mathcal{X}, D)$ be the coset in $\mathrm{Div}(\mathcal{X}, D)$ of divisors of degree m. Let $P(\mathcal{X}, D)$ be the subgroup of $\mathrm{Div}(\mathcal{X})$ of principal divisors of rational functions wich are 1 at P_i for all i. The *generalized Picard goup* is by definition the quotient group $\mathrm{Div}(\mathcal{X}, D)/P(\mathcal{X}, D)$ and will be denoted by $\mathrm{Pic}(\mathcal{X}, D)$. On the Picard group we have a well defined degree map, by taking the degree of a representing divisor. The inverse image of m under the degree map is denoted by $\mathrm{Pic}_m(\mathcal{X}, D)$. The group $\mathrm{Pic}_0(\mathcal{X}, D)$ is finite and is also called the *generalized class group* or *generalized Jacobian* of the curve, and its cardinality will be denoted by $h(\mathcal{X}, D)$, see [10].
The sets $\mathrm{Pic}_m(\mathcal{X}, D)$ are cosets of $\mathrm{Pic}_0(\mathcal{X}, D)$ and therefore they all have the same cardinality $h(\mathcal{X}, D)$. The class in $\mathrm{Pic}(\mathcal{X}, D)$ of a divisor $G \in \mathrm{Div}(\mathcal{X}, D)$ we will denote by $[G]_D$. In case $n = 0$, we denote $\mathrm{Div}(\mathcal{X}, D)$, $\mathrm{Pic}(\mathcal{X}, D)$, $[G]_D$ and $h(\mathcal{X}, D)$, respectively, by $\mathrm{Div}(\mathcal{X})$, $Pix(\mathcal{X})$, $[G]$ and $h(\mathcal{X})$, respectively.

Proposition 7.2 *If $n > 0$, then*

$$h(\mathcal{X}, D) = (q-1)^{n-1} h(\mathcal{X})$$

Proof Consider the well-defined map

$$\psi : \mathrm{Pic}_0(\mathcal{X}, D) \longrightarrow \mathrm{Pic}_0(\mathcal{X}) \ ; \ \psi([G]_D) = [G].$$

The map ψ is surjective by the independence of valuations. On the other hand, if $G \in \mathrm{Div}(\mathcal{X}, D)$ and $[G] = 0$, then $G = (f)$ for some rational function f, so $f(P_i) \neq 0$, for all i, since G has disjoint support with D. Now, given two classes of principal divisors in $\mathrm{Div}(\mathcal{X}, D)$, say of the rational functions f_1 and f_2, we have $[(f_1)] = [(f_2)]$ if and only if there exists a nonzero element $\lambda \in \mathbf{F}_q$ such that $f_1(P_i) = \lambda f_2(P_i)$ for every $i = 1, .., n$. Notice that for every n-tuple $\lambda_1, ..., \lambda_n$ of nonzero elements in $\mathbf{F}_q$ there exists a function f such that $f(P_i) = \lambda_i$ by the independence of valuations again. Thus we conclude that $Ker(\psi) \cong (\mathbf{F}_q^*)^n / \mathbf{F}_q^*$. $\square$

Definition 7.3 Let m be an integer such that $2g - 2 < m < n$. Let $SAG_m(\mathcal{X}, D)$ be the set of strongly algebraic geometric codes arising from divisors G of degree m, that is the set of codes of the form $C(D, G)$ on $\mathcal{X}$ on $\mathcal{X}$, where G is a divisor of degree m with disjoint support with D, see [8].

Corollary 7.4 *If $n > 2g + 2$ and $2g - 1 < m < n - 1$, then*

$$\#SAG_m(\mathcal{X}, D) = h(\mathcal{X}, D) = (q-1)^{n-1} h(\mathcal{X})$$

Proof If $n > 2g+2$ and $2g-1 < m < n-1$, then every $[G] \in \mathrm{Pic}_m(\mathcal{X}, D)$ gives a unique code $C(D, G)$, by Theorem 4.14. So the desired result follows from Proposition 7.2. $\square$

Definition 7.5 Let $\mathrm{Div}_m^+(\mathcal{X})$ be the set of effective divisors on $\mathcal{X}$ of degree m, and $a_m(\mathcal{X})$ be its cardinality. The *Zeta function* of $\mathcal{X}$ over $\mathbf{F}_q$ is defined as the power series

$$Z(\mathcal{X})(t) = \sum_{m=0}^{\infty} a_m(\mathcal{X}) t^m.$$

Now we can consider for every integer $m \geq 0$ the set $\mathrm{Div}_m^+(\mathcal{X}, D)$ of effective diviosrs in $\mathrm{Div}_m(\mathcal{X}, D)$ and let $a_m(\mathcal{X}, D)$ be its cardinality. The *generalized Zeta function* of $\mathcal{X}$ over $\mathbf{F}_q$ with respect to D is defined by

$$Z(\mathcal{X}, D)(t) = \sum_{m=0}^{\infty} a_m(\mathcal{X}, D) t^m.$$

Proposition 7.6

$$Z(\mathcal{X}, \mathbf{F}_q, \mathcal{P})(t) = (1-t)^n Z(\mathcal{X}, \mathbf{F}_q)(t).$$

Proof Denote $a_m(\mathcal{X})$ by a_m and $a_m(\mathcal{X}, D)$ by $\overline{a}_m$. From the definition of a_m and $\overline{a}_m$ we have the relation

$$a_m = \overline{a}_m + \overline{a}_{m-1} \#\{P_i \mid 1 \leq i \leq n\} + \overline{a}_{m-2} \#\{P_i + P_j \mid 1 \leq i \leq j \leq n\} + ...$$

Thus

$$a_m = \sum_{i=0}^{m} \binom{n+i-1}{i} \overline{a}_{m-i}.$$

Therefore

$$\overline{a}_m = \sum_{i=0}^{m} (-1)^i \begin{pmatrix} n \\ i \end{pmatrix} a_{m-i}.$$

If we substitute the above expression for $\overline{a}_m$ in the definition of $Z(\mathcal{X}, D)(t)$, than change the order of the double sum, and finally use Newton's binomium for $(1-t)^n$, then we get the desired formula. □

Corollary 7.7

$$h(\mathcal{X}) = (q-1) Res_{t=1} Z(\mathcal{X})(t).$$

If $n > 0$, then

$$h(\mathcal{X}, D) = (1-q)^n Res_{t=1} \frac{Z(\mathcal{X}, D)(t)}{(t-1)^n}.$$

Proof This follows from the fact that $Z(\mathcal{X})(t)$ is a rational function of the form

$$Z(\mathcal{X})(t) = \frac{P(t)}{(1-t)(1-qt)},$$

where $P(t)$ is a polynomial in t, and $h(\mathcal{X}) = P(1)$, see [14, 16], and Propositions 7.2 and 7.6. □

References

[1] Y. Driencourt, Some properties of elliptic codes over a field of characteristic 2, AAECC-3 Grenoble 1985, Lect. Notes Computer Sc. **229**, Springer-Verlag, Berlin Heidelberg New York, 1986, 185-193.

[2] Y. Driencourt and J.F. Michon, Rapport sur les codes géométriques, oct. 1986.

[3] Y. Driencourt and J.F. Michon, Remarques sur les codes géométriques, C.R. Acad. Sc. Paris **301** (1985), 15-17.

[4] Y. Driencourt and H. Stichtenoth, A criterion for self-duality of geometric codes, Communications in Algebra **17** (1989), 885-898.

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

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

[7] V.D. Goppa, Geometry and codes, Mathematics and its applications **24**, Kluwer Ac. Publ., Dordrecht, 1989.

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

[9] W. Scharlau, Selbstduale Goppa codes, Math. Nachr. **143** (1989), 119-122.

[10] J.-P. Serre, Groupes algébriques et corps de classes, Hermann, Paris, 1959. Tranlation: Algebraic goups and class fields, Grad. Texts Math. **117**, Springer-Verlag, Berlin Heidelberg New York, 1988.

[11] H. Stichtenoth, Self-dual Goppa codes, J. Pure Appl. Algebra **55** (1988), 199-211.

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

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

[14] H. Stichtenoth, Function fields in one variable and geometric Goppa codes, to appear in Universitext of Springer-Verlag.

[15] H.J. Tiersma, Codes comming from Hermitian curves, IEEE Trans. Inform. Theory IT-**33** (1987), 605-609.

[16] M.A. Tsfasman and Vlăduţ, Algebraic-geometric codes, Mathematics and its Applications **58**, Kluwer Acad. Publ., Dordrecht, 1991.

[17] C.-P. Xing, When are two geometric Goppa codes equal ?, IEEE Trans. Information Theory IT-**38** (1992), 1140-1142.