On the order bounds for one-point AG codes*

Olav Geil and Diego Ruano

Department of Mathematical Sciences
Aalborg University
Fr. Bajersvej 7G, 9220 Aalborg Øst, Denmark

Carlos Munuera

Department of Applied Mathematics
University of Valladolid
Avda Salamanca SN, 47014 Valladolid, Castilla, Spain

Fernando Torres

Institute of Mathematics, Statistics and Computer Science
P.O. Box 6065, University of Campinas
13083-970, Campinas, SP, Brazil

Abstract

The order bound for the minimum distance of algebraic geometry codes was originally defined for the duals of one-point codes and later generalized for arbitrary algebraic geometry codes. Another bound of order type for the minimum distance of general linear codes, and for codes from order domains in particular, was given in [1]. Here we investigate in detail the application of that bound to one-point algebraic geometry codes, obtaining a bound d^* for the minimum distance of these codes. We establish a connection between d^* and the order bound and its generalizations. We also study the improved code constructions based on d^*. Finally we extend d^* to all generalized Hamming weights.

1 Introduction

Algebraic geometry codes, or AG codes, over the finite field $\mathbb{F}_q$ with q elements are constructed from a (projective, non-singular, geometrically irreducible) algebraic curve $\mathcal{X}|\mathbb{F}_q$ and two rational divisors with disjoint support, $D = P_1 + \cdots + P_n$ and G . The code $C(D, G)$ is defined as the image of the Riemann-Roch space $\mathcal{L}(G)$ by the evaluation at D map $ev_D : \mathcal{L}(G) \to \mathbb{F}_q^n$, $ev_D(f) = (f(P_1), \ldots, f(P_n))$, see Section 3 or [3, 10, 14]. The divisor G is often taken as a multiple of a single point, $G = mQ$, with $Q \notin \mathrm{supp}(D)$. In this case $C(D, G) = C(D, mQ)$ is called *one-point* code.

*This work was supported in part by Danish National Science Research Council Grant FNV-21040368, the Danish FNU grant 272-07-0266, Junta de CyL under grant VA065A07 and by Spanish Ministry for Science and Technology under grants MTM2007-66842-C02-01 and MTM 2007-64704.

Given a code $C(D, mQ)$ the first task is to compute its parameters: length, dimension and minimum distance. The length is obviously $n = \deg(D)$. In order to compute the dimension an important role is played by the Weierstrass semigroup at Q,

$$H = H(Q) := \{-v_Q(f) : f \in \mathcal{L}(\infty Q) \setminus \{0\}\} = \{h_1 = 0 < h_2 < \dots\}$$

where v_Q is the valuation at Q and $\mathcal{L}(\infty Q) = \cup_{r=0,1,\dots}\mathcal{L}(rQ)$. In fact, if $h_i < n$ then the dimension of $C(D, h_iQ)$ is i. For $m \geq n$ this is no longer true in general, as the evaluation map $ev_D : \mathcal{L}(mQ) \to \mathbb{F}_q^n$ might have a non-trivial kernel, $\mathcal{L}(mQ - D)$. Thus we consider the set

$$H^* = H^*(D, Q) := \{m \in \mathbb{N}_0 : C(D, mQ) \neq C(D, (m-1)Q)\}.$$

Knowing H^* is equivalent to knowing the dimension of all codes $C(D, mQ)$. It is clear that H^* consists of n elements, that $H^* \subset H$ and that for $m < n$, $m \in H^*$ if and only if $m \in H$.

Regarding the minimum distance $d = d(C(D, mQ))$ the simplest estimate is given by the Goppa bound, $d \geq n - m$. The Goppa bound does not give the true minimum distance in many cases. For example, it does not give any information when $m \geq n$. This problem can be solved by using the improved Goppa bound, $d \geq n - m + \gamma_{a+1}$, where $a = \ell(mQ - D)$ is the *abundance* of $C(D, mQ)$. The drawback of this improved bound is that it is based on the gonality sequence (γ_i) of the curve $\mathcal{X}$, see [11], which is difficult to compute.

Besides uniform bounds, some of the most interesting known bounds for d are of order type. These bounds are based on obtaining different estimates for different subsets of codewords. They are successful if for each subset we can find estimates better than a uniform bound for all codewords, see [4]. The original order bound d_{ORD} (also called *Feng-Rao* bound) was introduced by Feng and Rao in [7] and by Høholdt, van Lint and Pellikaan in [10]. It usually gives very good results, but it has the disadvantage that it can only be applied to the duals of one-point codes, which are not one-point codes in general. A nice generalization of this bound for arbitrary AG codes was given by Beelen [2] and later improved by Duursma, Kirov and Park in a sequence of articles [4, 6, 5].

Another bound of order type for *general* linear codes was given in [1]. This bound was applied to order domain codes and to one-point codes in particular. In the present work, we investigate in detail the case of one-point codes, obtaining a bound d^*. This bound was already present in [1] (Proposition 37) but here we state it explicitly, by showing how to compute d^* from the set H^* defined above. Besides we investigate the connection to the order bound. We show that d^* is a special case of the Beelen and Duursma-Kirov-Park generalized bouds. Since it can happen that the generalized order bounds give different results than the original one, we also investigate the connection of d^* to the original order bound d_{ORD}. We show that when both can be applied -namely when the dual of a one-point code is isometric to a one-point code- then both coincide. Furthermore we investigate how to construct improved codes from d^* and how to extend d^* to all generalized Hamming weights. These problems have never been treated in the aforementioned works of Beelen and Duursma-Kirov-Park. Thus the main purpose of this article is not to present a new or better bound, but (i) to make the conection between the Andersen-Geil bound and the order bounds for AG one-point codes, (ii) to emphasize the possibility of manage the order

bound entirely in the language of one-point evaluation codes and Weierstrass semigroups; (iii) to study how to construct improved codes; and (iv) to extend d^* to all generalized Hamming weights.

The paper is structured in 5 sections: In Section 2 we briefly recall the bound for the minimum distance of linear codes from [1] as well as the main facts and definitions we need. We introduce the bound d^* for one-point codes in Section 3, where we also show the connection with the generalized order bounds of Beelen and Duursma-Kirov-Park. We also deal with improved codes, whose construction becomes now very easy. Some worked examples where we show how to compute d^* are included. In Section 4 we compare the bound d^* to the strict order bound (that is the original order bound d_{ORD} with respect to the evaluation map ev_D), showing that when both can be applied then they give the same result. Furthermore, we continue our study of improved codes. Finally in Section 5 we extend d^* to all generalized Hamming weights.

2 The bound from [1] for the minimum distance of linear codes

For the convenience of the reader, we begin with a brief explanation of some results from [1]. Let $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ be a basis of $\mathbb{F}_q^n$. We consider the codes $C_0 = (0)$, and for $i = 1, \ldots, n$,

$$C_i = \langle \mathbf{b}_1, \ldots, \mathbf{b}_i \rangle.$$

Associated to these codes we consider the (valuation-like) map $\nu : \mathbb{F}_q^n \to \{0, \ldots, n\}$ defined by $\nu(\mathbf{v}) = \min\{i : \mathbf{v} \in C_i\}$.

Lemma 2.1. *Let $\mathbf{v}_1, \ldots, \mathbf{v}_m \in \mathbb{F}_q^n$. Then*

(a) $\nu(\mathbf{v}_1 + \cdots + \mathbf{v}_m) \leq \max\{\nu(\mathbf{v}_1), \ldots, \nu(\mathbf{v}_m)\}$. *If there exists j such that $\nu(\mathbf{v}_i) < \nu(\mathbf{v}_j)$ for all $i \neq j$, then equality holds.*

(b) $\dim(\langle \mathbf{v}_1, \ldots, \mathbf{v}_m \rangle) \geq \#\{\nu(\mathbf{v}_1), \ldots, \nu(\mathbf{v}_m)\}$. *Conversely, if $D \subseteq \mathbb{F}_q^n$ is a linear subspace of dimension m, then there exists a basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ of D such that $\#\{\nu(\mathbf{v}_1), \ldots, \nu(\mathbf{v}_m)\} = m$.*

Proof. (a) is clear. (b) Assume $\#\{\nu(\mathbf{v}_1), \ldots, \nu(\mathbf{v}_m)\} = t$ and $\nu(\mathbf{v}_1) < \cdots < \nu(\mathbf{v}_t)$. If $\lambda_1\mathbf{v}_1 + \cdots + \lambda_t\mathbf{v}_t = 0$ then $0 = \nu(\mathbf{0}) = \nu(\lambda_1\mathbf{v}_1 + \cdots + \lambda_t\mathbf{v}_t) = \max\{\nu(\mathbf{v}_i) : \lambda_i \neq 0\}$. By (a) this implies $\lambda_1 = \cdots = \lambda_t = 0$. Conversely write $D_i = D \cap C_i$. For all $i = 1, \ldots, n$, it holds that $D_i = D_{i-1} \oplus (D \cap \langle \mathbf{b}_i \rangle)$, hence $\dim(D_{i-1}) \leq \dim(D_i) \leq \dim(D_{i-1}) + 1$ and the last inequality is an equality precisely m times. If $D_i \neq D_{i-1}$, take a vector $\mathbf{v}_i \in D_i \setminus D_{i-1}$. Then $\#\{\nu(\mathbf{v}_1), \ldots, \nu(\mathbf{v}_m)\} = m$ and according to (b), $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ is a basis of D. □

For $\mathbf{c} \in \mathbb{F}_q^n$, $\mathbf{c} \neq 0$, we consider the space $V(\mathbf{c}) = \{\mathbf{v} \in \mathbb{F}_q^n : \mathrm{supp}(\mathbf{v}) \subseteq \mathrm{supp}(\mathbf{c})\} = \{\mathbf{v} * \mathbf{c} : \mathbf{v} \in \mathbb{F}_q^n\}$, where the component-wise product is defined as usual: $\mathbf{v} * \mathbf{c} = (v_1c_1, \ldots, v_nc_n)$. Clearly $\dim(V(\mathbf{c})) = \mathrm{wt}(\mathbf{c})$, where $\mathrm{wt}(\mathbf{c})$ denotes the weight of $\mathbf{c}$. Now consider in $\{1, \ldots, n\}^2$ the order $(r, s) < (i, j)$ if and only if $r \leq i$, $s \leq j$ and $(r, s) \neq (i, j)$. A pair $(\mathbf{b}_i, \mathbf{b}_j)$ is called *well-behaving* if $\nu(\mathbf{b}_r * \mathbf{b}_s) < \nu(\mathbf{b}_i * \mathbf{b}_j)$ for all $(r, s) < (i, j)$. For $i = 1, \ldots, n$, define

$$\Lambda_i = \{\mathbf{b}_j \in \mathcal{B} : (\mathbf{b}_i, \mathbf{b}_j) \text{ is well-behaving}\}.$$

Since we can write $\mathbf{c} = \lambda_1 \mathbf{b}_1 + \cdots + \lambda_{\nu(\mathbf{c})} \mathbf{b}_{\nu(\mathbf{c})}$ with $\lambda_{\nu(\mathbf{c})} \neq 0$, then for $\mathbf{b}_j \in \Lambda_{\nu(\mathbf{c})}$ we have

$$\nu(\mathbf{c} * \mathbf{b}_j) = \nu(\sum_{i=1}^{\nu(\mathbf{c})} \lambda_i \mathbf{b}_i * \mathbf{b}_j) = \nu(\mathbf{b}_{\nu(\mathbf{c})} * \mathbf{b}_j).$$

Proposition 2.2. *Let $\mathbf{c} \in \mathbb{F}_q^n$. If $\mathbf{c} \neq \mathbf{0}$ then $\mathrm{wt}(\mathbf{c}) \geq \#\Lambda_{\nu(\mathbf{c})}$.*

Proof. We have $\mathrm{wt}(\mathbf{c}) = \dim(V(\mathbf{c})) \geq \dim(\langle \mathbf{c} * \mathbf{b}_1, \ldots, \mathbf{c} * \mathbf{b}_n \rangle) \geq \#\{\nu(\mathbf{c} * \mathbf{b}_1), \ldots, \nu(\mathbf{c} * \mathbf{b}_n)\} \geq \#\{\nu(\mathbf{c} * \mathbf{b}_j) : j \in \Lambda_{\nu(\mathbf{c})}\} = \#\{\nu(\mathbf{b}_{\nu(\mathbf{c})} * \mathbf{b}_j) : j \in \Lambda_{\nu(\mathbf{c})}\} = \#\Lambda_{\nu(\mathbf{c})}$. □

Theorem 2.3. *For $i = 1, \ldots, n$, the true minimum distance of C_i, satisfies $d(C_i) \geq \min\{\#\Lambda_r : r \leq i\}$.*

This bound can be applied to an arbitrary linear code C, just by including it into an increasing chain of codes $C_1 \subset \cdots \subset C_{k-1} \subset C \subset C_{k+1} \subset \cdots \subset C_n = \mathbb{F}_q^n$. Such a chain is quite natural for one-point codes.

3 A bound for the minimum distance of one-point codes

3.1 The bound

Let $\mathcal{X}$ be a (projective, non-singular, geometrically irreducible algebraic) curve of genus g defined over the finite field $\mathbb{F}_q$. We construct one-point codes from $\mathcal{X}$ in the usual way. Let $Q, P_1, \ldots, P_n$ be different rational points in $\mathcal{X}$. Let $v = -v_Q$, where v_Q is the valuation at Q, and consider the spaces $\mathcal{L}(mQ)$ and the algebra $\mathcal{L}(\infty Q) = \cup_{r=0,1,\ldots} \mathcal{L}(rQ)$. Let $D = P_1 + \cdots + P_n$ and $ev = ev_D : \mathcal{L}(\infty Q) \to \mathbb{F}_q^n$ be the evaluation map at D. The one-point codes $C(D, mQ)$ arising from $\mathcal{X}, D$ and Q are defined as the images of the sets $\mathcal{L}(mQ)$ by ev, that is $C(D, mQ) = ev(\mathcal{L}(mQ))$. Note that $C(D, (n + 2g - 1)Q) = \mathbb{F}_q^n$, hence we can restrict ourselves to $0 \leq m \leq n + 2g - 1$.

Let $C = C(D, mQ)$. We shall apply to C the bound from Section 2 with respect to the sequence of codes $C_1 \subset C_2 \subset \cdots \subset C_n$, obtained from the sequence $(C(D, mQ))_{m=0,\ldots,n+2g-1}$ by deleting the repeated codes. Thus the map ν can be written as

$$\nu(\mathbf{v}) = \min\{\dim(C(D, mQ)) : \mathbf{v} \in C(D, mQ)\}.$$

From now on, unless explicitly said, we restrict ourselves to codes with length $n > 2g + 2$.

Lemma 3.1. *For $f \in \mathcal{L}(\infty Q)$ we have $\nu(ev(f)) \leq \dim(C(D, v(f)Q))$. If $C(D, v(f)Q) \neq C(D, (v(f)-1)Q)$ then equality holds, $\nu(ev(f)) = \dim(C(D, v(f)Q))$.*

Proof. The first statement is clear since $f \in \mathcal{L}(v(f)Q)$ and hence $ev(f) \in C(D, v(f)Q)$. For the second one, note that if $m = v(f)$, then $\mathcal{L}(mQ) = \mathcal{L}((m-1)Q) + \langle f \rangle$, and hence $C(D, mQ) = C(D, (m-1)Q) + \langle ev(f) \rangle$. Thus $ev(f) \in C(D, mQ) \setminus C(D, (m-1)Q)$. □

Note that it is not true in general that $\nu(ev(f)) = \dim(C(D, v(f)Q))$ because ev only depends on the points $P_1, \ldots, P_n$, and thus $ev(f)$ might be equal to $ev(g)$ with $g \in C(D, (v(f)-1)Q)$. For example, take a non-constant function $f \in \mathcal{L}(\infty Q)$. Then $v(f^q) = qv(f)$ but $ev(f^q) = ev(f)$.

Let $H = H(Q) = \{h_1 = 0 < h_2 < \ldots\}$ be the Weierstrass semigroup of Q. As we know, this is a numerical semigroup of finite genus g. Let $l_1, \ldots, l_g$ be the gaps of H. Let us consider the set H^* defined in the Introduction, namely

$$H^* = H^*(D, Q) := \{m \in \mathbb{N}_0 : C(D, mQ) \neq C(D, (m-1)Q)\}.$$

It is clear that H^* consists of n elements. Let us write $H^* = \{m_1, \ldots, m_n\}$. It is also clear that $H^* \subset H$ and for $m < n$ it holds that $m \in H^*$ if and only if $m \in H$. The following results may be useful for computing H^*. Remember that for a divisor E, $\ell(E)$ stands for the dimension of $\mathcal{L}(E)$.

Proposition 3.2. *$H^* = \{m \in H : \ell(mQ - D) = \ell((m-1)Q - D)\}$.*

Proof. If $m < n$ then $C(D, mQ) \neq C(D, (m-1)Q)$ if and only if $m \in H$ that is if and only if $m \in H^*$. If $m \geq n$ then the kernel of the evaluation map restricted to $\mathcal{L}(mQ)$ is $\ker(ev|_{\mathcal{L}(mQ)}) = \mathcal{L}(mQ - D)$. Since $m-1, m \in H$, then $C(D, mQ) \neq C(D, (m-1)Q)$ if and only if both kernels are equal. □

Thus, for $m \geq n$, and since $\ell((n + 2g - 1)Q - D) = g$ and H has g gaps, we conclude that g elements of $\{n, \ldots, n + 2g - 1\}$ belong to H^* while the other g elements do not.

Corollary 3.3. *Let $m \geq n$. If $m \notin H^*$ then for all $h \in H$ it holds that $m + h \notin H^*$.*

Proof. If $m \notin H^*$ then there exists a non-zero function $f \in \mathcal{L}(mQ - D) \setminus \mathcal{L}((m-1)Q - D)$. Take a function $\phi \in \mathcal{L}(hQ)$ such that $v(\phi) = h$. Then $f\phi \in \mathcal{L}((m+h)Q - D) \setminus \mathcal{L}((m+h-1)Q - D)$, and hence $m + h \notin H^*$. □

Corollary 3.4. *If the divisors D and nQ are linearly equivalent, $D \sim nQ$, then $H^* \cap \{n, \ldots, n + 2g - 1\} = \{n + l_1, \ldots, n + l_g\}$, hence $H^* = (H \cap \{1, \ldots, n-1\}) \cup \{n + l_1, \ldots, n + l_g\}$.*

Proof. If $D \sim nQ$ then $n \notin H^*$ and hence, according to Corollary 3.3, $n = n + h_1, \ldots, n + h_g \notin H^*$. The statement follows by cardinality reasons. □

Let $f \in \mathcal{L}(\infty Q)$. If $v(f) \in H^*$ then, by Lemma 3.1, we have $\nu(ev(f)) = \dim(C(v(f)))$. For $i = 1, \ldots, n$, let $f_i \in \mathcal{L}(\infty Q)$ be such that $v(f_i) = m_i$. Thus, according to Lemma 2.1 (b), $\mathcal{B} = \{ev(f_1), \ldots, ev(f_n)\}$ is a basis of $\mathbb{F}_q^n$ and the sequence of codes (C_i) is given by

$$C_i = \langle ev(f_1), \ldots, ev(f_i)\rangle = C(D, m_i Q),\ i = 1, \ldots, n.$$

Our sequence $(C(D, m_i Q))$ does not contain the code $C_0 = (0)$. If we want to include it (see Section 4 for example) we simply take $m_0 = -1$ and $C(D, m_0 Q) = (0)$.

Proposition 3.5. *If $m_i + m_j \in H^*$ then $(ev(f_i), ev(f_j))$ is a well behaving pair.*

Proof. For $\phi_1, \phi_2 \in \mathcal{L}(\infty Q)$ we have that $v(\phi_1\phi_2) = v(\phi_1) + v(\phi_2)$. If $m_i + m_j \in H^*$ then $\nu(ev(f_i) * ev(f_j)) = \nu(ev(f_i f_j)) = \dim(C(D, v(f_i f_j)Q)) = \dim(C(D, (m_i + m_j)Q))$. If $(r, s) < (i, j)$ then $v(f_r f_s) < v(f_i f_j)$ and hence $\nu(ev(f_r) * ev(f_s)) = \nu(ev(f_r f_s)) < \dim(C(D, (m_i + m_j)Q))$. □

Thus from the bound in Section 2 we get a bound for one-point codes as follows. For $i = 1, \ldots, n$, consider the sets

$$\Lambda_i^* = \{m \in H^* : m = m_i + m_j \text{ with } m_j \in H^*\}.$$

If $m \in m_i + H \setminus H^*$ then $m = m_i + h$ for some $h \in H \setminus H^*$ and thus $m \notin H^*$ according to Corollary 3.3. Thus the sets Λ_i^* can also be written as $\Lambda_i^* = \{m \in H^* : m - m_i \in H\} = (m_i + H) \cap H^*$. According to Propositions 2.2 and 3.5, we have that $\mathrm{wt}(\mathbf{c}) \geq \#\Lambda_r^*$ for all $\mathbf{c} \in C(D, m_r Q) \setminus C(D, m_{r-1}Q)$. Define

$$d^*(i) := \min\{\#\Lambda_r^* : r \leq i\}.$$

Then $d(C(D, m_i Q)) \geq d^*(i)$, or equivalently

Theorem 3.6. *For a non-negative integer m, we have $d(C(D, mQ)) \geq d^*(\dim(C(D, mQ)))$.*

We call this inequality the d^* *bound* for one-point codes. Let us remember that the classical bound on the minimum distance of an code is given by the Goppa estimate $d(C(D, mQ)) \geq d_G(C(D, mQ)) := n - m$. d^* improves the Goppa bound as the next result shows (see also Proposition 37 in [1]). The first element in $H \setminus H^*$ is denoted by $\pi = \pi(H)$. Note that $\pi \geq n$.

Proposition 3.7. *For all $i = 1, \ldots, n$, we have $d^*(i) \geq d_G(C(D, m_i Q))$. If $m_i < \pi - l_g$ then equality holds, $d^*(i) = d_G(C(D, m_i Q))$.*

Proof. For the first statement it suffices to show that $\#(H^* \setminus \Lambda_r^*) \leq m_r$ for all r. Since $\Lambda_i^* = (m_i + H) \cap H^*$, we have $H^* \setminus \Lambda_i^* \subseteq H \setminus (m_i + H)$ and this follows from the fact that $\#(H \setminus (m_r + H)) = m_r$ (see [10], Lemma 5.15). If $m_i + l_g < \pi$, then all elements in $H \setminus (m_i + H)$ are smaller than π and hence $H^* \setminus \Lambda_i^* = H \setminus (m_i + H)$. □

3.2 d^* and the generalized order bounds of Beelen and Duursma-Kirov-Park

The bound d^* can also be obtained from the generalized order bounds of Beelen and Duursma-Kirov-Park. Let us show first how to get d^* from the Beelen generalized order bound d_B stated in [2]. Let $m_i \in H^*$ and consider the code $C(D, m_i Q)$. The Beelen bound applies to the duals of evaluation codes. Thus, let W be a canonical divisor with simple poles and residue 1 at all points $P \in \mathrm{supp}(D)$ and let $G = D + W - m_i Q$. It is well known that $C(D, m_i Q) = C(D, G)^\perp$ (see [14]). By using the notation as in [2], for $r = 0, 1, 2, \ldots$, consider the divisors

$$F^{(r)} := G + rQ = F_1^{(r)} + F_2^{(r)} =: (D + W) + ((r - m_i)Q).$$

Note that all the divisors $F^{(r)}, F_1^{(r)}, F_2^{(r)}$ above have support disjoint from D. For a divisor E, let $H(Q,E)$ be the Weierstrass set of Q relative to E,

$$H(Q,E) = -v_Q\left(\bigcup_{\deg(E+sQ)\geq 0} \mathcal{L}(E+sQ)\setminus\{0\}\right).$$

In our case, for all $r = 0,1,\ldots,$ we have $H(Q,F_2^{(r)}) = H(Q,(r-m_i)Q) = H(Q,0) = H$, the usual Weierstrass semigroup of Q. The Beelen bound states that

$$d(C(D,m_iQ)) \geq \min\{\#N(F_1^{(r)},F_2^{(r)}) : r = 0,1,\ldots\}$$

where

$$\begin{aligned} N(F_1^{(r)},F_2^{(r)}) &= \{(t,s) : t\in H(Q,F_1^{(r)}), s\in H(Q,F_2^{(r)}), t+s = v_Q(G)+1\} \\ &= \{(t,s) : t\in H(Q,D+W), s\in H, t+s = 1-m_i\}. \end{aligned}$$

According to the Rieman-Roch theorem, for an integer m it holds that $1-m\in H(Q,D+W)$ if and only if $\ell(mQ-D) = \ell((m-1)Q-D)$. Thus for $m\in H$ the conditions $m\in H^*$ and $1-m\in H(Q,D+W)$ are equivalent. Consequently

$$\begin{aligned} \#N(F_1^{(r)},F_2^{(r)}) &= \#\{s\in H : 1-(s+m_i)\in H(Q,F_1^{(r)})\} \\ &= \#\{s\in H : s+m_i\in H^*\} \end{aligned}$$

as $s\in H$ implies $s+m_i\in H$. Finally observe that while the sets Λ_i^* and $\{s\in H : s+m_i\in H^*\}$ count different objects, they are of the same cardinality: the map $m\mapsto m+m_i$ gives a bijection from Λ_i^* to $\{s\in H : s+m_i\in H^*\}$. Thus, for one-point codes, the bound d^* can be seen as a particular case of the Beelen bound d_B, relative to the choice of $Q,Q,\ldots$ as infinite sequence of points not in $\mathrm{supp}(D)$ and the divisors $F_1^{(r)} = D+W, F_2^{(r)} = (r-m_i)Q$. In particular in may happen that $d^* < d_B$ (for an accurate choice of the infinite sequence of points and the divisors $F_1^{(r)}, F_2^{(r)}$), in the same way as it may happen that $d_{ORD} < d_B$ (see Example 8 of [2]).

Let us show briefly how to obtain d^* from the generalized order bound of Duursma, Kirov and Park. Consider again the code $C(D,m_iQ)$. In the formulation of [4, 6, 5], if $\mathbf{c}\in C(D,m_iQ)\setminus C(D,m_{i-1}Q)$, then

$$\mathrm{wt}(\mathbf{c}) \geq \#(\Delta_Q(D-m_iQ)\cap\{(m-m_i)Q : m\geq m_i\})$$

where for a divisor E, $\Delta_Q(E)$ is defined as

$$\Delta_Q(E) = \{A : \mathcal{L}(A)\neq\mathcal{L}(A-Q), \mathcal{L}(A-E)\neq\mathcal{L}(A-Q-E)\}.$$

The same argument as in the case of d_B proves that the sets Λ_i^* and $(\Delta_Q(D-m_iQ)\cap\{(m-m_i)Q : m\geq m_i\})$ are of the same cardinality. This shows that d^* can also be obtained from the extended Duursma-Kirov-Park order bound.

On the other hand, the choice of the sets Λ_i^* (instead of the counting made in the Beelen and Duursma-Kirov-Park bounds) has some technical advantages. Firstly it does not involve more divisors that the ones naturally associated to the code $C(D,mQ)$. And secondly, in contrast to what happens with those bounds, d^* allows us to study improved codes very easily. Also it allows us to extend the same idea to all generalized Hamming weights (see Section 5). In fact, for these two problems d^* works even better than the original order bound d_{ORD}. As discussed in Section 4, d^* extends exactly d_{ORD} to one-point codes.

3.3 Improved codes

Let δ be an integer, $0 < \delta \leq n$. In the same way as the order bound allows us to construct codes with designed minimum distance δ and dimension as large as possible, see [10], the bound d^* shows how to construct similar codes from sequences $(C(D, m_i Q))$, see [1]. Specifically, given δ let us consider the *improved code*

$$C(D, Q, \delta) = \langle \{ ev(f_i) : \#\Lambda_i^* \geq \delta \} \rangle$$

where $f_i \in \mathcal{L}(\infty Q)$ with $v(f_i) = m_i$. From Lemma 2.1 (a), and the discussion before Theorem 3.6, it is clear that the minimum distance of $C(D, Q, \delta)$ is at least δ.

The sequence (Λ_i^*) is said to be *monotone* for δ if for every i, j such that $\#\Lambda_i^* \geq \delta$ and $\#\Lambda_j^* < \delta$ we have that $i < j$. If (Λ_i^*) is monotone for δ it is clear that $C(D, Q, \delta)$ is a usual one-point code, so improved codes only improve one-point codes for those δ for which the sequence is not monotone. In this case the code $C(D, Q, \delta)$ depends on the choice of the set $\{f_1, \ldots, f_n\}$. In fact, if $\#\Lambda_i^* = \delta$ and $\#\Lambda_j^* < \delta$ for some $j < i$, then $v(f_i + f_j) = v(f_i)$ but in general $ev(f_j) \notin C(D, Q, \delta)$, hence $ev(f_i + f_j) \notin C(D, Q, \delta)$. Thus we have a collection of improved codes with designed distance δ, depending on the collection of sets $\{f_1, \ldots, f_n\}$.

3.4 Worked examples

We compute H^* for some examples.

Example 3.8. (Codes on Castle curves) A curve $\mathcal{X}$ defined over $\mathbb{F}_q$ is said to be *Castle* if there is a rational point Q such that the Weierstrass semigroup at Q, $H = H(Q)$, is symmetric and $qh_2 + 1 = \#\mathcal{X}(\mathbb{F}_q)$ (where h_2 is the first nonzero element of H). If D is the sum of all rational points of $\mathcal{X}$ except Q, the codes $C(D, mQ)$ are called Castle codes, see [13]. It is simple to see that for Castle curves we have $D \sim nQ$, hence $H^* \cap \{n, \ldots, n + 2g - 1\} = \{n + l_1, \ldots, n + l_g\}$ according to Proposition 3.4. In Section 4 we shall see that, being the semigroup H symmetric, we have $H^* = H \setminus (n + H)$. Recall that the family of Castle codes includes Hermitian, generalized Hermitian, Norm-trace, Suzuki, Ree and many of the most known codes. To study a concrete example, let us consider the Suzuki curve $\mathcal{X}$ over $\mathbb{F}_8$ (see [13] again). This curve has genus $g = 14$ and 65 rational points. A plane model of $\mathcal{X}$ is given by the equation $Y^8 Z^2 - Y Z^9 = X^2(X^8 - X Z^7)$. This model is non-singular except at the point $(0 : 1 : 0)$. Being this singularity uni-branched, the unique point Q lying over $(0 : 1 : 0)$ is rational. Let us consider the codes $C(D, mQ)$, where D is the sum of all rational points of $\mathcal{X}$ except Q. The Weierstrass semigroup at Q is known to be $H = \langle 8, 10, 12, 13 \rangle$. A straightforward computation gives the sequence $(\#\Lambda_i^*)$: (64, 56, 54, 50, 49, 48, 46, 44, 43, 42, 41, 40, 38, 36, 35, 34, 33, 32, 31, 30, 29, 28, 28, 26, 26, 24, 23, 22, 21, 20, 21, 18, 20, 16, 18, 16, 14, 13, 14, 10, 14, 8, 13, 10, 10, 9, 9, 6, 9, 8, 4, 6, 5, 5, 4, 6, 5, 3, 2, 3, 3, 2, 1, 1).

This sequence is monotone for $\delta = 3, 5, 6, 9, 13, 14, 18, 20, 21$. For example the code $C(D, 70Q)$ has dimension 55 and distance at least 4 (that is $d^*(55) = 4$), whereas $C(D, Q, 4)$ has dimension 57.

Example 3.9. (Two families of codes from a curve over $\mathbb{F}_{16}$) The computation of H^* for long codes can be carried often to the computation of H^* for much

shorter codes. Let $C(D, mQ)$ be a code and let n'' be the largest integer for which equality in the Goppa bound holds. Then $n'' < n$ and there exists a divisor $D'' \leq D$ such that $D'' \sim n''Q$. Hence, for $m \geq n$ we have $\ell(mQ - D) = \ell((m - n'')Q - D')$ where $D' = D - D''$. This leads us to considering the codes $C(D', m'Q)$ of length $n' = n - n''$. To give an example of this situation let us consider the curve $\mathcal{X}$ over $\mathbb{F}_{16}$ defined by the affine equation

$$y^{15} = p(x) := \frac{x(x^{14} - 1)}{x - 1} = x^{14} + x^{13} + \cdots + x.$$

Let us study the rational points of $\mathcal{X}$. Firstly there is just one point Q over $x = \infty$. Regarding the affine points, note that the polynomial $p(x)$ has 2 roots in $\mathbb{F}_{16}$, namely 0 and 1. In fact, if $\alpha \neq 0, 1$ is a root of $p(x)$, then $\alpha^7 = 1$ and $7 \nmid 15$. These roots give two points, $R_1 = (0, 0)$ and $R_1 = (1, 0)$. We consider now the morphism $\phi = x$, $\phi : \mathcal{X} \to \mathbb{P}^1(\overline{\mathbb{F}}_{16})$ of order 15, where $\overline{\mathbb{F}}_{16}$ denotes the algebraic closure of $\mathbb{F}_{16}$. For $\alpha \in \mathbb{F}_{16}$, $\alpha \neq 0, 1$, from the equation of $\mathcal{X}$, we have $y^{15} = \alpha(\alpha^{14} - 1)/(\alpha - 1) = 1$, so that there are 15 rational points over each $\phi(\alpha)$. Write

$$\operatorname{div}(x - \alpha) = \sum_{i=1}^{15} P_\alpha^i - 15Q.$$

Thus $\mathcal{X}$ has $(16 - 2) \cdot 15 + 2 + 1 = 213$ rational points. To compute its genus observe that

$$y^{15} = x(x - 1)(x - \alpha_1)^2 \dots (x - \alpha_6)^2,$$

where $\alpha_i^7 \neq 1$, $\alpha_i \notin \mathbb{F}_{16}$. As the extension $\mathbb{F}_{16}(\mathcal{X})|\mathbb{F}_{16}(x)$ is Kummer, the genus can be computed via the Riemann-Hurwitz formula [14],

$$2g - 2 = 15(-2) + 9(14) = 96$$

and $g = 49$. Note that $\mathcal{X}$ attains the record of rational points among all curves genus 49 over $\mathbb{F}_{16}$. Finally let us compute the Weierstrass semigroup H at Q. We have seen that $-v_Q(x) = 15$. In the same way $\operatorname{div}_\infty(y) = 14Q$, so $14, 15 \in H$. Let

$$z := y^8/((x - \alpha_1) \cdots (x - \alpha_6)).$$

It is easy to compute $\operatorname{div}_\infty(z) = 22Q$, hence $22 \in H$ and thus $\langle 14, 15, 22\rangle \subseteq H$. Since both semigroups have equal genus we conclude that equality holds. Then

$$\begin{aligned} H(Q) = \langle 14, 15, 22\rangle = \{&0, 14, 15, 22, 28, 29, 30, 36, 37, 42, 43, 44, 45, 50, 51, 52, 56, 57,\\ &58, 59, 60, 64, 65, 66, 67, 70, 71, 72, 73, 74, 75, 78, 79, 80, 81, 82, 84, 85, 86, 87,\\ &88, 89, 90, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, \dots\}. \end{aligned}$$

Note that $2g - 1 = 97 \in H$ and so H is not symmetric. In order to construct codes from this curve let us consider the divisors $D' = R_1 + R_2$, and for $\alpha \in \mathbb{F}_{16}$, $\alpha \neq 0, 1$

$$D''_\alpha = \sum_{i=1}^{15} P_\alpha^i \ , \ D'' = \sum_\alpha D''_\alpha.$$

According to our previous computations, $D''_\alpha \sim 15Q$ and hence $D'' \sim 210Q$. Let $D = D' + D''$ be the sum of all affine points of $\mathcal{X}$, $n = 212 = \deg(D)$ and consider the codes of length n, $C(D, mQ)$, $m = 0, \dots, n + 2g - 1 = 309$. In order

to determine $H^* = H^*(D, Q)$ we have to compute $\ell(mQ - D)$ for $m \geq n$. But since $D'' \sim 210Q$, then $\ell(mQ - D) = \ell((m - 210)Q) - D')$. This fact leads us to considering the codes $C(D', m'Q)$ for $m' = 2, \ldots, 2g + 1 = 99$. The length of these codes is $n' = 2$ and $C(D', 0Q) = \langle (1, 1) \rangle$. Thus there exists just one m' for which the dimension increases. Clearly, this is not the case for any gap of H, so m' must be a non-gap. Looking at the generator matrix $(1, 1)$ of $C(D', 0Q)$ we conclude that this m' is the smallest order of a function f in $\mathcal{L}(\infty Q)$ such that $f(R_1) \neq f(R_2)$. Such a function is clearly $f = x$ and hence $m' = 15$. Thus,

$$H(D, Q)^* \cap \{n, \ldots, n+2g-1\} = \{n-2+l : \ l \text{ is a gap of } H \text{ and } l \geq 2\} \cup \{n-2+15\}.$$

Once H^* is known we can compute the dimensions of all codes $C(D, mQ)$ and apply Theorem 3.6 to estimate the minimum distances. Note that for large m we do not obtain good parameters. In fact, as $D''_\alpha \sim 15Q$, for all $m < n$, m multiple of 15, the true minimum distance of $C(D, mQ)$ equals the Goppa estimate. In particular the minimum distance distance of $C(D, 210Q)$ is $d = 2$. The bound d^* gives $d \geq 2$ for $m = 224$ (that is, for dimension $k \leq 175$) and hence all codes $C(D, mQ)$, $m = 210, \ldots, 224$ have true minimum distance $d = 2$.

In order to obtain codes with better parameters (that is, better minimum distance) the usual approach is to consider another divisor G. We shall show that this goal can also be accomplished by taking a slightly different D. Consider the codes $C(D'', mQ)$ of length $n'' = 210$. Then the function from which the codeword of weight 2 arises belongs to the kernel of the evaluation map. The set $H^* = H^*(D'', Q)$ can be now computed by using Corollary 3.4, and $H^* \cap \{n'', \ldots, n'' + 2g - 1\} = \{n'' + l_1, \ldots, n'' + l_g\}$, where $l_1, \ldots, l_g$ are the 49 gaps of H. It is not necessary to apply the bound d^* to see that the minimum distance of these codes is larger for $m \geq n''$. For example, from the improved Goppa bound we know that the minimum distance of $C(D'', 210Q)$ satisfies $d \geq n'' - 210 + \gamma_2 = \gamma_2$, where γ_2 is the usual gonality of $\mathcal{X}$, see [11] . It is not easy to compute γ_2, but at the first sight we have $\gamma_2 \geq \#\mathcal{X}(\mathbb{F}_{16})/\#\mathbb{P}^1(\mathbb{F}_{16})$, hence $\gamma_2 \geq 13$ (so $\gamma_2 = 13$ or 14) and $d \geq 13$ as well.

4 Relating the bounds d^* and d_{ORD}

As we noted above, in some cases the generalized order bounds may give different results than the original order bound, see [2] Example 8. Likewise, also the Andersen-Geil bound, from which we have obtained d^*, can be very different from the original order bound, see Example 51 of [1]. In this Section we shall compare d^* and the original order bound d_{ORD}. This comparison can be done over sequences of one-point codes such that their duals are also one-point. We can slightly relax this condition by imposing that the duals are isometric to one-point codes.

4.1 The isometry-dual condition

Let C, D, be two linear codes in $\mathbb{F}_q^n$ and let $\mathbf{x} \in (\mathbb{F}_q^*)^n$ be an n-tuple of non-zero elements. We say that C and D are *isometric* according to $\mathbf{x}$ (or simply $\mathbf{x}$-*isometric*) if the map $\chi_{\mathbf{x}} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ given by $\chi_{\mathbf{x}}(\mathbf{v}) = \mathbf{x} * \mathbf{v}$ satisfies $\chi_{\mathbf{x}}(C) = D$. Note that $\chi_{\mathbf{x}}$ is a true linear isometry for the Hamming distance, hence isometric codes have the same parameters. The dual of a code C is denoted by $C^\perp$.

Proposition 4.1. *Let C, D be two linear codes in $\mathbb{F}_q^n$. If $\chi_{\mathbf{x}}(C) = D$ then $\chi_{\mathbf{x}}(D^\perp) = C^\perp$.*

Proof. Let $\mathbf{c} \in C$ and $\mathbf{d} = \chi_{\mathbf{x}}(\mathbf{c}) \in D$. For all $\mathbf{v} \in \mathbb{F}_q^n$ we have $\mathbf{v}\cdot\mathbf{d} = \mathbf{v}\cdot(\mathbf{x}*\mathbf{c}) = (\mathbf{x}*\mathbf{v})\cdot\mathbf{c}$, hence $\mathbf{v} \in D^\perp$ if and only if $\chi_{\mathbf{x}}(\mathbf{v}) \in C^\perp$. □

Let us recall that we have fixed a basis $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ of $\mathbb{F}_q^n$ and the associated codes $C_i = \langle \mathbf{b}_1, \ldots, \mathbf{b}_i \rangle$, $i = 0, \ldots, n$.

Definition 4.2. A sequence of codes $(C_i)_{i=0,\ldots,n}$ is said to satisfy the *isometry-dual* condition if there exists $\mathbf{x} \in (\mathbb{F}_q^*)^n$ such that C_i is $\mathbf{x}$-isometric to $C_{n-i}^\perp$ for all $i = 0, 1, \ldots, n$.

Let us study the case of AG codes. We consider the sequence of codes $(C(D, m_iQ))_{i=0,\ldots,n}$ arising from the curve $\mathcal{X}$ and the associated set $H^* = \{m_1, \ldots, m_n\}$. In addition let $m_0 = -1$ and $C(D, m_0Q) = (0)$. If $(C(D, m_iQ))$ satisfies the isometry-dual condition then both d^* and the order bound d_{ORD} can be used to estimate the minimum distance of these codes. Let us remember that we are assuming that $n > 2g + 2$. Remember also that the dual of $C(D, mQ)$ is $C(D, D + W - mQ)$, where W is a canonical divisor with simple poles and residue 1 at every point in $\mathrm{supp}(D)$ (see [14]).

Proposition 4.3. *The following statements are equivalent.*

(a) *The sequence $(C(D, m_iQ))_{i=0,\ldots,n}$ satisfies the isometry-dual condition.*

(b) *The divisor $(n + 2g - 2)Q - D$ is canonical.*

(c) *$n + 2g - 1 \in H^*$.*

Proof. Let us consider the divisor $E = (n + 2g - 2)Q - D$ and for an integer m write $m^\perp = n + 2g - 2 - m$. ((a)⇔(b)) Assume that the sequence $(C(D, m_iQ))_{i=0,\ldots,n}$ satisfies the isometry-dual condition. Let m be such that $2g \leq m \leq n-2$ (since $n > 2g+2$, such an m does exist). Then $2g \leq m^\perp \leq n-2$ and hence $m, m^\perp \in H^*$. In particular $\dim(C(D, mQ)) + \dim(C(D, m^\perp Q)) = n$. Since the sequence $(C(D, m_iQ))_{i=0,\ldots,n}$ satisfies the isometry-dual condition we have that $C(D, D + W - mQ) = C(D, mQ)^\perp$ is isometric to $C(D, m^\perp Q)$. This implies that the divisors $D + W - mQ$ and $m^\perp Q$ are equivalent (see [12]). Then $W \sim (m + m^\perp)Q - D = E$ and this divisor is canonical. Conversely, if E is a canonical divisor then there is a rational function f such that $E + \mathrm{div}(f) = W$. In particular f has neither poles nor zeros in $\mathrm{supp}(D)$. Let $\mathbf{x} = ev_D(f)$. Then we have $D + W - mQ = m^\perp Q + \mathrm{div}(f)$ hence $C(D, mQ)^\perp = \mathbf{x} * C(D, m^\perp Q) = \chi_{\mathbf{x}}(C(D, m^\perp Q)$. ((b)⇔(c)) Since $\deg(E) = 2g - 2$, then E is canonical if and only if $\ell(E) = g$. By the Riemann-Roch theorem (see [10], Theorem 2.55), we have $\ell(E + Q) = g$ hence E is canonical if and only if $\ell(E) = \ell(E + Q)$, that is, if and only if $n + 2g - 1 \in H^*$ according to Proposition 3.2 □

Example 4.4. (Codes on Castle curves) Let $\mathcal{X}$ be a Castle curve and $(C(D, m_iQ))_{i=0,\ldots,n}$ be a sequence of Castle codes of length n arising from $\mathcal{X}$ (see Example 3.8). Since $D \sim nQ$ and the semigroup $H(Q)$ is symmetric, Proposition 3.4 implies that $(C(D, m_iQ))_{i=0,\ldots,n}$ satisfies the isometry-dual condition.

Example 4.5. (Codes on the Klein quartic) Let us consider the Klein quartic $\mathcal{X}$ of projective equation $X^3Y + Y^3Z + Z^3X = 0$ and genus $g = 3$. Over the field $\mathbb{F}_8$, $\mathcal{X}$ has 24 rational points (the maximum allowed by Weil-Serre bound) and a rich geometrical structure. Codes coming from this curve are usually constructed by using the divisors $G = m(Q_1 + Q_2 + Q_3)$, where $Q_1 = (1 : 0 : 0), Q_2 = (0 : 1 : 0)$ and $Q_3 = (0 : 0 : 1)$, since this choice has some technical advantages (see [3],[8],[10]). However, one-point codes over $\mathcal{X}$ can also be considered. Let $Q = Q_2$, $D' = Q_1 + Q_3$, $D'' = P_1 + \cdots + P_{21}$ be the sum of all rational points except Q_1, Q_2, Q_3 and let $D = D' + D''$. It is easy to see that $\mathrm{div}(x) = 3Q_3 - 2Q_2 - Q_1$ and $\mathrm{div}(y) = 2Q_1 + Q_3 - 3Q_2$. Then $\mathrm{div}(xy) = Q_1 + 4Q_3 - 5Q_2$ and $\mathrm{div}(x^2y) = 7Q_3 - 7Q_2$. Then the Weierstrass semigroup $H = H(Q)$ is generated by 3,5 and 7. In particular $\{1, y, xy, y^2, x^2y, \dots\}$ is a basis of $\mathcal{L}(\infty Q)$. In order to compute $H^* = H^*(D, Q)$ we can proceed as in Example 3.9. By considering the morphism $\phi = y$, $\phi : \mathcal{X} \to \mathbb{P}^1(\overline{\mathbb{F}}_8)$ of degree 3, we observe that $D'' \sim 21Q$. This fact leads us to consider the codes $C(D', mQ)$ of length 2 and the set $H^*(D', Q)$. Since x^2y is the first non constant function in the above basis for which Q_1 is not a zero, we deduce that $H^*(D', Q) = \{0, 7\}$. Then $21+7 = 28 = n+2g-1 \in H^*(D, Q)$ and the sequence of codes $C(D, m_iQ)$ satisfies the isometry-dual condition. As we shall se in Lemma 4.7, this condition provides the whole set H^* and $H^* = \{0, 3, 5, 6, 7, \dots, 22, 23, 25, 28\}$. A direct computation shows that for this sequence of codes, both d^* and the order bound give the true minimum distance for all m.

Example 4.6. Let us consider the sequence of codes of length $n = 212$ introduced in Example 3.9. Here $n+2g-1 = 309 \notin H^*$ hence this sequence does not satisfy the isometry-dual condition. As a consequence d_{ORD} cannot be applied to estimate the minimum distances.

4.2 The bounds for isometry dual codes

Let $(C(D, m_iQ))_{i=0,\dots,n}$ be a sequence of one-point codes satisfying the isometry-dual condition. For this sequence the set H^* is particularly simple and can be computed just in terms of the Weierstrass semigroup H.

Lemma 4.7. *If $(C(D, m_iQ))$ satisfies the isometry-dual condition, then $H^* = \{m \in H : n + 2g - 1 - m \in H\}$.*

Proof. Let $m \in H$. From the Riemann-Roch theorem, $\ell(mQ - D) = m - n + 1 - g + \ell((n + 2g - 2 - m)Q)$ and hence $\ell(mQ - D) = \ell((m - 1)Q - D)$ if and only if $\ell((n + 2g - 2 - m)Q) \neq \ell((n + 2g - 1 - m)Q)$, that is, if and only if $n + 2g - 1 - m \in H$. □

Thus for isometry-dual sequences the set H^* is symmetric in the sense that for an integer m it holds that $m \in H^*$ if and only if $n + 2g - 1 - m \in H^*$ (and conversely this property implies the isometry-dual condition). It follows that $n+2g-1-m_i = m_{n-i+1}$. We must not confuse this kind of symmetry with the symmetry of the semigroup H. Let us remember that a semigroup H of genus g is called *symmetric* if $2g-1 \notin H$ or equivalently (since its largest gap l_g satisfies $l_g \leq 2g - 1$) if $l_g = 2g - 1$. For symmetric semigroups it holds that $m \in H$ if and only if $l_g - m \notin H$, see [10]. When the Weierstrass semigroup $H = H(Q)$ is symmetric, $(2g - 2)Q$ is a canonical divisor, hence the isometry-dual property

is equivalent to $D \sim nQ$. Since in this case the condition $n + 2g - 1 - m \in H$ is equivalent to $m - n \notin H$, or $m \notin n + H$, then the set H^* is given by

$$H^* = H \setminus (n + H).$$

Let us return to the general case of H, where it might not be symmetric. The symmetrical description of H^* given by Lemma 4.7 allows us to write H^* in the following way

Proposition 4.8. *If the sequence $(C(D, m_iQ))$ satisfies the isometry-dual condition, then $H^* = \{0, \ldots, n+2g-1\} \setminus \{l_1, \ldots, l_g, n+2g-1-l_g, \ldots, n+2g-1-l_1\}$.*

Proof. We have $l_1, \ldots, l_g \notin H^*$. In the same way, if l is a gap of H then $n+2g-1-(n+2g-1-l) = l \notin H$ and hence $n+2g-1-l \notin H^*$. Furthermore, since $l_g < n$, then $l_g < n + 2g - 1 - l_g$ and hence $\#\{l_1, \ldots, l_g, n + 2g - 1 - l_g, \ldots, n + 2g - 1 - l_1\} = 2g$. By cardinality reasons we get the result. □

For $i = 1, \ldots, n$, let us consider the set $L_i = \{m_i + l_1, \ldots, m_i + l_g\}$.

Proposition 4.9. *If $(C(D, m_iQ))$ satisfies the isometry-dual condition, then $\#\Lambda_i^* = n - i + 1 - \#(L_i \cap H^*)$.*

Proof. Let $L = \{l_1, \ldots, l_g, n+2g-1-l_g, \ldots, n+2g-1-l_1\}$, and for $i = 1, \ldots, n$,

$$\begin{aligned} B_i^{(1)} &= \{m_j \in H^* : m_i + m_j < n + 2g, m_i + m_j \notin H^*\}, \\ B_i^{(2)} &= \{m_j \in H^* : m_i + m_j \geq n + 2g\}. \end{aligned}$$

Clearly $\#\Lambda_i^* = \#(H^* \setminus (B_i^{(1)} \cup B_i^{(2)})) = n - \#B_i^{(1)} - \#B_i^{(2)}$. Since $H^* \subseteq H$ and the sum of two non-gaps is again a non-gap, we have $B_i^{(1)} = \{m_j \in H^* : m_i + m_j \in L\} = \{n + 2g - 1 - l_g - m_i, \ldots, n + 2g - 1 - l_1 - m_i\} \cap H^*$. According to Lemma 4.7, $\#B_i^{(1)} = \#(L_i \cap H^*)$. Besides $\#B_i^{(2)} = i - 1$. In fact, if $m_i + m_j \geq n + 2g$, from Lemma 4.7 we can write $m_j = n + 2g - 1 - m_t$ with $t = n - j + 1$. Then $n + 2g - 1 + m_i - m_t > n + 2g - 1$ if and only if $m_i > m_t$ and there exist $i - 1$ such choices for m_t. □

Then d^* can be written for isometry-dual codes as

$$d(C(D, m_iQ)) \geq d^*(i) = \min\{n - r + 1 - \#(L_r \cap H^*) : r \leq i\}.$$

Let us prove now that d^* and the strict order bound with respect to the evaluation map ev_D, $d_{ORD,ev}$ ([10], Section 4.3), give the same result when applied to codes satisfying the isometry-dual condition. Let $m_i \in H^*$ and let us compute both bounds for $C(D, m_iQ)$. If $m_i < n - l_g$, according to Proposition 3.7 and Theorem 4.7 in [10], both bounds are equal to Goppa bound.

In order to compute the order bound, we first need the duals of the codes $C(D, m_rQ)$. As we know, $C(D, m_rQ)^\perp$ is isometric to $C(D, (n+2g-2-m_r)Q)$. Let $h_s, h_{s+1} \in H$ be such that $h_s \leq n+2g-2-m_r < h_{s+1}$. Then $C(D, h_sQ) = C(D, (n + 2g - 2 - m_r)Q)$ and hence $C(D, h_sQ)^\perp$ is isometric to $C(D, m_rQ)$. Note that $C(D, m_rQ)$ has dimension r, so $C(D, h_sQ)$ has dimension $n - r$. Furthermore, Lemma 4.7 implies that $n + 2g - 1 - m_r \in H^*$ hence $h_{s+1} = n + 2g - 1 - m_r = m_{n-r+1}$ and $\dim C(D, h_{s+1}Q) = n - r + 1$.

For $h \in H$ let us consider the set

$$A[h] = \{t \in H : h - t \in H\}.$$

The strict order bound on the minimum distance of $C(D, m_i Q)$ together with our previous discussion, imply that

$$\begin{aligned} & d(C(D, m_i Q)) \geq d_{ORD,ev}(C(D, m_i Q)) \\ := & \min\{\#A[h] : h \in H^*, h \geq n + 2g - 1 - m_i\} \\ = & \min\{\#A[n + 2g - 1 - m_r] : m_r \in H^*, r \leq i\} \\ = & \min\{\#A[m_{n-r+1}] : r \leq i\}, \end{aligned}$$

where the last two equalities follow from 4.7 and the fact that $m_{n-r+1} = n + 2g - 1 - m_r$.

Lemma 4.10. *If $h \in H$ and $l \notin H$ then $l - h \notin H$.*

Proof. If $l - h = h' \in H$ then $l = h + h'$ and hence $l \in H$. □

Proposition 4.11. *Let $m_r \in H^*$. If $(C(D, m_i Q))$ satisfies the isometry-dual condition, then $\#\Lambda_r^* = \#A[m_{n-r+1}]$.*

Proof. Let us compute $\#A[n + 2g - 1 - m_r] + \#(L_r \cap H^*)$. For a given gap l of H, we have $m_r + l \in H^*$ if and only if $n + 2g - 1 - m_r - l \in H^*$. Thus

$$\begin{aligned} \#(L_r \cap H^*) &= \#\{l \in \mathrm{Gaps}(H) : n + 2g - 1 - m_r - l \in H^*\} \\ &= \#\{h \in H^* : n + 2g - 1 - m_r - h \in \mathrm{Gaps}(H)\}, \end{aligned}$$

so $\#A[n+2g-1-m_r]+\#(L_r \cap H^*) = \#\{h \in H : h \leq n+2g-1-m_r\} - \#\{h \in H \setminus H^* : h \leq n+2g-1-m_r, n+2g-1-m_r-h \in \mathrm{Gaps}(H)\}$. Let us note that for all $h \in H \setminus H^*$, $h \leq n+2g-1-m_r$, it holds that $n+2g-1-h \in \mathrm{Gaps}(H)$. In fact, according to Lemma 4.7, we would otherwise have $h \in H^*$. Then, from Lemma 4.10, $n + 2g - 1 - m_r - h \in \mathrm{Gaps}(H)$. So $\{h \in H \setminus H^* : h \leq n+2g-1-m_r, n+2g-1-m_r-h \in \mathrm{Gaps}(H)\} = \{h \in H \setminus H^* : h \leq n+2g-1-m_r\}$ and hence $\#A[n+2g-1-m_r]+\#(L_r \cap H^*) = \#\{h \in H^* : h \leq n+2g-1-m_r\} = \dim(C(D, (n + 2g - 1 - m_r)Q)) = n - r + 1$. □

Corollary 4.12. *For isometry-dual codes, we have $d_{ORD,ev}(C(D, m_i Q)) = d^*(i)$.*

Therefore d^* and the strict order bound are the same for isometry-dual codes.

4.3 More on improved codes

In Section 3.3 we have considered the improved code $C(D, Q, \delta) = \langle\{ev(f_i) : \#\Lambda_i^* \geq \delta\}\rangle$, for $1 \leq \delta \leq n$. It is analogous to the improved code $\tilde{C}(D, Q, \delta)$ introduced by Feng and Rao, [7, 10], based on the order bound:

$$\tilde{C}(D, Q, \delta) = \langle\{ev(f_i) : \#A[m_i] < \delta\}\rangle^{\perp}.$$

It is well known that the minimum distance of $\tilde{C}(D, Q, \delta)$ is at least δ. When the sequence $(C(D, m_i Q))$ is isometry-dual, Proposition 4.11 allows us to write $\tilde{C}(D, Q, \delta)$ in terms of the sets Λ_i^*'s,

$$\tilde{C}(D, Q, \delta) = \langle\{ev(f_i) : \#\Lambda_{n+1-i}^* \geq \delta\}\rangle^{\perp}.$$

Then it is natural to wonder about the relation between these two improved codes $\tilde{C}(D,Q,\delta)$ and $C(D,Q,\delta)$.

Proposition 4.13. *If the sequence $(C(D,m_iQ))$ satisfies the isometry-dual condition, then $C(D,Q,\delta)$ and $\tilde{C}(D,Q,\delta)$ have the same dimension.*

Proof. If $C(D,Q,\delta)$ is generated by t vectors then $\tilde{C}(D,Q,\delta)$ is defined by $n-t$ independent parity checks. □

If the sequence (Λ_i^*) is monotone for δ then $C(D,Q,\delta)$ is a one-point code, hence $C(D,Q,\delta)$ and $\tilde{C}(D,Q,\delta)$ are isometric. Let us study the general case.

Lemma 4.14. *Let $(C_i = \langle \mathbf{b}_1,\ldots,\mathbf{b}_i\rangle)$ be a sequence of codes that satisfies the isometry-dual condition, $\chi_{\mathbf{x}}(C_i) = C_{n-i}^{\perp}$. Then for $i = 1,2,\ldots,n$, we have*

$$\chi_{\mathbf{x}}(\mathbf{b}_i) \in C_{n-i}^{\perp} \setminus C_{n-i+1}^{\perp}.$$

Proof. Follows directly from the definition of isometry-dual sequence. □

Let us remember that the improved codes $C(D,Q,\delta)$ and $\tilde{C}(D,Q,\delta)$ depend on the choice of functions $f_1,\ldots,f_n$ in $\mathcal{L}(\infty Q)$ such that $v(f_i) = m_i$.

Lemma 4.15. *If $(C(D,m_iQ))$ satisfies the isometry-dual condition then given a set $\{f_1,\ldots,f_n\}$ of functions in $\mathcal{L}(\infty Q)$ with $v(f_i) = m_i$, there exists a similar set $\{f_1',\ldots,f_n'\}$ such that $\chi_{\mathbf{x}}(ev(f_i'))\cdot ev(f_j) \neq 0$ holds if and only if $j = n-i+1$.*

Proof. By Lemma 4.14 and the isometry-dual condition, the sets $\{f_1,\ldots,f_n\}$ and $\{f_1',\ldots,f_n'\}$ will satisfy

$$\begin{array}{ll} (\chi_{\mathbf{x}}(ev(f_i')))\cdot ev(f_j) = 0 & \text{for } \ j = 1,\ldots,n-i \\ (\chi_{\mathbf{x}}(ev(f_i')))\cdot ev(f_{n-i+1}) \neq 0. & \end{array}$$

So, we have to determine a particular set $\{f_1',\ldots,f_n'\}$ that in addition satisfies

$$(\chi_{\mathbf{x}}(ev(f_i')))\cdot ev(f_j) = 0 \qquad \text{for} \qquad j = n-i+2,\ldots,n. \tag{1}$$

We show the existence of such a set by induction. Note first that given arbitrary $\{f_1,\ldots,f_n\}$ then the condition (1) is trivially satisfied for $i=1$ if we choose $f_1' = f_1$. Assume next that (1) holds for all values of $i = 1,\ldots,s$, where s is some number less than n. That is, for each $i \in \{1,\ldots,s\}$ the only j such that $\chi_{\mathbf{x}}(ev(f_i'))\cdot ev(f_j) \neq 0$ is $j = n-i+1$. Denote by a_j the value of $\chi_{\mathbf{x}}(ev(f_i'))\cdot ev(f_j)$, $j = n-s+1,\ldots,n$. The function

$$f_{s+1}' = f_{s+1} - \sum_{i=1}^{s} \frac{a_i}{\chi_{\mathbf{x}}(ev(f_i'))\cdot ev(f_{n+1-i})} f_i'$$

satisfies (1) as

$$\chi_{\mathbf{x}}(ev(f_{s+1}'))\cdot ev(f_j) = \chi_{\mathbf{x}}(ev(f_{s+1}))\cdot ev(f_j) - \left(\sum_{i=1}^{s} \frac{a_i}{\chi_{\mathbf{x}}(ev(f_i'))\cdot ev(f_{n-i+1})}\chi_{\mathbf{x}}(ev(f_i'))\cdot ev(f_j)\right).$$

□

Proposition 4.16. *Assume* $\big(C(D, m_1Q)\big)$ *satisfies the isometry-dual condition. For every choice of* $\{f_1, \ldots, f_n\}$ *of functions in* $\mathcal{L}(\infty Q)$ *with* $v(f_i) = m_i$*, there exists a similar set* $\{f'_1, \ldots f'_n\}$ *such that the code* $\tilde{C}(D, Q, \delta)$ *defined from the first set is isometric to the code* $C(D, Q, \delta)$ *defined from the latter set. A similar result holds the other way around.*

Proof. By Propositions 4.9 and 4.11 we have $\#\Lambda_i^* = \#A[m-n+1-i]$. Choosing $\{f'_1, \ldots, f'_n\}$ such that Lemma 4.15 is satisfied and applying the definitions of $C(D, Q, \delta)$ and $\tilde{C}(D, Q, \delta)$ proves the first claim. The last claim follows by symmetry. □

5 Generalized Hamming weights

The same ideas used to obtain the bound d^* for the minimum distance can be applied to all generalized Hamming weights (see [1]). Let us remember that given a set $D \subseteq \mathbb{F}_q^n$, the *support* of D is defined as

$$\mathrm{supp}(D) = \bigcup_{\mathbf{v} \in D} \mathrm{supp}(\mathbf{v}).$$

Let C be a code of dimension k. For $r = 1, \ldots, k$, the r-th *generalized Hamming weight* of C is defined as

$$d_r(C) = \min\{\#\mathrm{supp}(D) : D \text{ is an } r\text{-dimensional linear subspace of } C\},$$

and the sequence $d_1(C), \ldots, d_k(C)$, is called the *weight hierarchy* of C. Let us first look a general bound on the $d_r(C)$'s. Recall that we have a basis $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ of $\mathbb{F}_q^n$ and codes $C_i = \langle \mathbf{b}_1, \ldots, \mathbf{b}_i \rangle$.

Lemma 5.1. *Let* $D \subseteq \mathbb{F}_q^n$ *be a linear subspace of dimension* r *and let* $\{\mathbf{c}_1, \ldots, \mathbf{c}_r\}$ *be a basis of* D*. Then* $\#supp(D) \geq \#\cup_{i=1,\ldots,r} \{\nu(\mathbf{b}_{\nu(\mathbf{c}_i)} * \mathbf{b}_j) : j \in \Lambda_{\nu(\mathbf{c}_i)}\}$.

Proof. Given D, let us consider the space $V(D) = \{\mathbf{v} \in \mathbb{F}_q^n : \mathrm{supp}(\mathbf{v}) \subseteq \mathrm{supp}(D)\}$. Since $\#\mathrm{supp}(D) = \dim(V(D))$ and $\mathrm{supp}(D) = \mathrm{supp}(\mathbf{c}_1) \cup \cdots \cup \mathrm{supp}(\mathbf{c}_r)$, we have that $V(D) = V(\mathbf{c}_1) + \cdots + V(\mathbf{c}_r)$ and the statement follows from the results in Section 2. □

Theorem 5.2. *For* $r = 1, \ldots, i$*, the* r*-th generalized Hamming weight of* C_i *satisfies*

$$d_r(C_i) \geq \min_{1 \leq j_1 < \cdots < j_r \leq i} \# \left\{ \bigcup_{j \in \{j_1, \ldots, j_r\}} \{\nu(\mathbf{b}_j * \mathbf{b}_t) : t \in \Lambda_j\} \right\}.$$

Proof. According to Lemma 2.1 (c), every linear subspace D of C_i has a basis $\{\mathbf{c}_1, \ldots, \mathbf{c}_r\}$ such that $1 \leq \nu(\mathbf{c}_1) < \cdots < \nu(\mathbf{c}_r) \leq i$. Conversely, given vectors $\{\mathbf{c}_1, \ldots, \mathbf{c}_r\}$ satisfying the above condition, $\langle \mathbf{c}_1, \ldots, \mathbf{c}_r \rangle$ is a vector subspace of C_i of dimension r. Then the result is a consequence of Lemma 5.1. □

This result is easily translated to one-point AG codes. With the notation as in Section 3, we have codes $C(D, mQ)$ and $C_i = C(D, m_iQ)$. We showed that $\#\{\nu(\mathbf{b}_j * \mathbf{b}_t) : t \in \Lambda_j\}) \geq \#\Lambda_j^*$. Thus we have

Theorem 5.3. *Let m be a non-negative integer. For $r = 1, \ldots, i = \dim(C(D, mQ))$, the r-th generalized Hamming weight of $C(D, mQ)$ satisfies*

$$d_r(C(D, mQ)) \geq d_r^*(i) := \min_{1 \leq j_1 < \cdots < j_r \leq i} \#(\Lambda_{j_1}^* \cup \cdots \cup \Lambda_{j_r}^*).$$

This result is similar to the corresponding one for the order bound in [9]. Also similar results to the ones contained in this section can be obtained for improved codes as well.

Acknowledgments

The authors wish to thank Peter Beelen and Tom Høholdt for hospitality and interesting discussions on the subject. This paper was written in part during a visit of the second author to Aalborg University and The Technical University of Denmark. He wishes to thank both institutions for hospitality and support. We also wish to thank Iwan M. Duursma, Radoslav Kirov and Seungkook Park for supporting us with the idea behind the material in Section 3.2.

References

[1] H. Andersen and O. Geil, *Evaluation codes from order domain theory*, Finite Fields Appl., **14** (2008), 92–123.

[2] P. Beelen, *The order bound for general algebraic geometric codes*, Finite Fields Appl., **13** (2007), 665–680.

[3] I. Duursma, *Algebraic geometry codes: general theory*, in "Advances in Algebraic Geometry Codes" (eds. E. Martinez-Moro, C. Munuera and D. Ruano), World Scientific, Hackensack, (2008), 1–48.

[4] I. Duursma and R. Kirov, *An extension of the order bound for AG codes*, in "Applied Algebra, Algebraic Algorithms and Error-Correcting Codes" (eds. M. Bras and T. Hoholdt), (2009), 11–22.

[5] I. Duursma, R. Kirov and S. Park, *Distance bounds for algebraic geometric codes*, preprint, arXiv1001.1374

[6] I. Duursma and S. Park, *Coset bounds for algebraic geometric codes*, Finite Fields Appl., **16** (2010pp. 36–55.

[7] G. L. Feng and T. N. T. Rao, *Improved geometric Goppa codes. Part I: basic theory*, IEEE Trans. Inform. Theory, **41** (1995pp. 1678–1693.

[8] J. Hansen, *Codes on the Klein quartic, ideals, and decoding*, IEEE Trans. Inform. Theory, **33** (1987), 923–925.

[9] P. Heijnen and R. Pellikaan, *Generalized Hamming weights of q-ary Reed-Muller codes*, IEEE Trans. Inform. Theory, **44** (1998), 181–197.

[10] T. Høholdt, J. H. van Lint and R. Pellikaan, *Algebraic geometry codes*, in "Handbook of Coding Theory" (eds. V.S. Pless, W.C. Huffman and R.A. Brualdi), Elsevier, Amsterdam, The Netherlands, (1998), 871–961.

[11] C. Munuera, *Generalized Hamming weights and trellis complexity*, in "Advances in Algebraic Geometry codes" (eds. E. Martinez-Moro, C. Munuera and D. Ruano), World Scientific, Hackensack, (2008), 363–390.

[12] C. Munuera and R. Pellikaan, *Equality of geometric Goppa codes and equivalence of divisors*, J. Pure Appl. Algebra, **90** (1993), 229–252.

[13] C. Munuera, A. Sepúlveda and F. Torres, *Algebraic geometry codes from Castle curves*, in "Coding Theory and Applications" (ed. Á. Barbero), Springer, (2008), 117–127.

[14] H. Stichtenoth, "Algebraic Function Fields and Codes," Springer, New York, 1993.

E-mail address: olav@math.aau.dk
E-mail address: cmunuera@arq.uva.es
E-mail address: diego@math.aau.dk
E-mail address: ftorres@ime.unicamp.br