Which linear codes are algebraic-geometric ?

R. Pellikaan, B.-Z. Shen and G.J.M. van Wee *

Appeared in: IEEE Trans. Inform. Theory. IT-**37** (1991), 583-602.

Abstract

An infinite series of curves is constructed in order to show that all linear codes can be obtained from curves using Goppa's construction. If one imposes conditions on the degree of the divisor used, then we derive criteria for linear codes to be algebraic-geometric. In particular, we investigate the family of q-ary Hamming codes, and prove that only those with redundancy one or two, and the binary $[7, 4, 3]$ code are algebraic-geometric in this sense. For these codes we explicitly give a curve, rational points and a divisor. We prove that this triple is in a certain sense *unique* in the case of the $[7, 4, 3]$ code.

Key words: algebraic-geometric codes, algebraic curves, divisors, generalized Goppa codes, geometric Goppa codes.

I. Introduction

Since the early papers by Goppa [5],[6],[7], [8], algebraic-geometric codes have been in the spotlight of coding theoretic research for about a decade. As is well-known, numerous exciting results have been achieved using Goppa's construction of linear codes from algebraic curves over finite fields, both by algebraic geometrists and coding theorists. Because of the difficulty of the subject, several explanatory papers and text books have appeared, see for instance [9] or [16]. In this paper we investigate which linear codes can be constructed by Goppa's method. It turns out that it makes sense to distinguish between three types of codes, according to the degree of the divisor used in the construction. For more details, see Section II (Definition 2).

*All authors are with the Eindhoven University of Technology, Department of Mathematics and Computing Science, PO Box 513, 5600 MB Eindhoven, The Netherlands. This research was partially supported by the Netherlands organization for scientific research (NWO).

Although this paper is quite self-contained, a certain knowledge of algebraic geometry is taken for granted. For this, we refer to [2],[4],[11],[16] or [22]. For coding theory, see [15],[16] or [17].

Outline of the paper

In Section II we define *weakly algebraic-geometric* (WAG), *algebraic-geometric* (AG), and *strongly algebraic-geometric* (SAG) codes (Definition 2). The class of SAG codes is a proper subset of the class of AG codes, and the class of AG codes is a proper subset of the class of WAG codes. Furthermore, we also explain what we mean by a WAG, AG or SAG representation of a code. Some basic properties are mentioned. Section II actually serves as an introduction to the rest of the paper. At the end of Section II we introduce the notion of a *minimal* representation. We prove that every WAG, AG or SAG code of dimension at least two has a minimal WAG, AG or SAG representation, respectively. This is useful in Sections IV and V.

The WAG codes are the codes which can be obtained by Goppa's construction when no restrictions are imposed on the degree of the divisor used. Inspired by the notion of a covering curve of Goppa [9] and a paper by Hansen and Stichtenoth [10], we prove in Section III that *every* linear code is WAG. In this way we solve problem (3.1.19) of [22]. The curves are given explicitly. Goppa [7, p.78] claimed that every linear code is WAG, but his proof is not sufficient, see Remark 5. Lachaud [14, (5.10)] made a weaker claim, namely that every linear code is a subcode of a WAG code.

In Section IV we derive several conditions on linear codes to be AG. As proved at the end of that section, all binary SAG codes have length ≤ 8. By the results of Section III, the class of AG codes therefore seems to be the most interesting. Special attention is paid to Reed-Muller codes, Hamming codes and the binary Golay code and its extension. For example, the conditions on AG codes imply that a q-ary Hamming code of redundancy r is not AG if $r > 2$ and $(r, q) \neq (3, 2)$.

In Section V we are interested in explicit WAG, AG or SAG representations of codes, and in the question whether something can be said about the uniqueness of these representations. As an example, we investigate the family of q-ary Hamming codes in close detail (Section V-A). We prove that these codes are SAG in the cases left open in Section IV. In the case $(r, q) = (3, 2)$, that is, for the binary [7,4,3] code, we obtain the nice result that this code has a *unique* minimal representation as an AG code. In Section V-B we discuss another example, namely a code which was mentioned in [13], and prove that it is SAG.

Notation

We use $\mathbf{F}_q$ to denote the finite field of q elements. We use $\mathbf{P}^l$ to denote the l-dimensional projective space; it will be clear from the context over which field (usually $\mathbf{F}_q$ or the algebraic closure $\overline{\mathbf{F}_q}$). If any confusion is possible, we use $\mathbf{P}^l(\mathbf{F}_q)$ to denote the finite set of $(q^{l+1}-1)/(q-1)$ points over $\mathbf{F}_q$ in $\mathbf{P}^l$, for instance. Similarly, $\mathbf{A}^l$ denotes the l-dimensional affine space. By a curve over a field k we mean a projective, reduced scheme over k of dimension one. As with $\mathbf{P}^l$ and $\mathbf{A}^l$, we sometimes write $\mathcal{X}(\mathbf{F}_q)$ to indicate the finite set of

$\mathbf{F}_q$-rational points on $\mathcal{X}$. The function field of $\mathcal{X}$ over k is denoted by $k(\mathcal{X})$. The group of divisors on $\mathcal{X}$ is denoted by $\mathrm{Div}(\mathcal{X})$. If $\varphi : \mathcal{X} \to \mathcal{X}'$ is a morphism of curves, then we denote by φ^* both the induced homomorphism $k(\mathcal{X}') \to k(\mathcal{X})$ and the induced homomorphism $\mathrm{Div}(\mathcal{X}') \to \mathrm{Div}(\mathcal{X})$, see [11, p.137]. If $f \in k(\mathcal{X}) \setminus \{0\}$, we denote by (f) its divisor, a so-called *principal* divisor. The notation $\mathrm{div}(f)$ is also used in the literature. Similarly, if ω is a nonzero rational differential form on $\mathcal{X}$, then we denote its divisor by (ω), a so-called *canonical* divisor. If P is a place of $k(\mathcal{X})$ over k, that is a discrete valuation ring of $k(\mathcal{X})$ over k, then we denote by v_P the discrete valuation function at P. In the literature the notation ord_P is also customary. If D is a divisor on $\mathcal{X}$, then $\mathrm{supp}(D)$ denotes the *support* of D, that is the set of places with nonzero coefficient in D. If D_1 and D_2 are divisors on a curve $\mathcal{X}$, then we denote by $D_1 \sim D_2$ that D_1 and D_2 are linearly equivalent. By $[D]$ we denote the linear equivalence class of D, that is the set consisting of all the divisors on $\mathcal{X}$ linearly equivalent with D. The *complete linear system* associated to D is denoted by $|D|$. This is the set of all effective divisors in $[D]$. We denote by $Pic(\mathcal{X})$ the group of divisors on $\mathcal{X}$ modulo principal divisors, the so-called *divisor class group*. By $Pic_0(\mathcal{X})$ we denote the subgroup of $Pic(\mathcal{X})$ consisting of the divisors of degree 0 modulo principal divisors. By $Pic_m(\mathcal{X})$ we denote the coset of $Pic_0(\mathcal{X})$ in $Pic(\mathcal{X})$ consisting of the divisors of degree m modulo principal divisors. By $\mathcal{D}_m$ we denote the set of effective divisors on $\mathcal{X}$ of degree m. We define $h := \#Pic_0(\mathcal{X})$. In fact, we have $h = \#Pic_m(\mathcal{X})$ for every m. For all this, see [16].

If C is a linear code, we denote by $d(C)$ its minimum distance.

II. Algebraic-geometric codes and representations

Definition 1 Let $\mathcal{X}$ be a projective, nonsingular, absolutely irreducible curve defined over $\mathbf{F}_q$. The genus of $\mathcal{X}$ is denoted by $g(\mathcal{X})$, or simply by g, if it is clear which curve is meant. Let $P_1, \ldots, P_n$ be n distinct $\mathbf{F}_q$-rational points of $\mathcal{X}$. We denote both the n-tuple $(P_1, \ldots, P_n)$ and the divisor $P_1 + \ldots + P_n$ by D (the order of the P_i is fixed). Let G be a divisor on $\mathcal{X}$ of degree m with support disjoint from the support of D. Let $\mathbf{F}_q(\mathcal{X})$ be the function field of $\mathcal{X}$ over $\mathbf{F}_q$ and $L(G) = \{f \in \mathbf{F}_q(\mathcal{X})^* | (f) \geq -G\} \cup \{0\}$. Let $\Omega_{\mathcal{X}}$ be the vector space of rational differential forms on $\mathcal{X}$ and $\Omega(G) = \{\omega \in \Omega_{\mathcal{X}} \setminus \{0\} | (\omega) \geq G\} \cup \{0\}$. Define the map

$$\alpha_L : L(G) \longrightarrow \mathbf{F}_q^n,$$
$$\text{by} \quad \alpha_L(f) = (f(P_1), \ldots, f(P_n)),$$

and the map

$$\alpha_\Omega : \Omega(G - D) \longrightarrow \mathbf{F}_q^n,$$
$$\text{by} \quad \alpha_\Omega(\omega) = (res_{P_1}(\omega), \ldots, res_{P_n}(\omega)).$$

Define

$$C_L(\mathcal{X}, D, G) = \mathrm{Image}(\alpha_L) \quad \text{and} \quad C_\Omega(\mathcal{X}, D, G) = \mathrm{Image}(\alpha_\Omega).$$

We abbreviate $C_L(\mathcal{X}, D, G)$ and $C_\Omega(\mathcal{X}, D, G)$ by $C_L(D, G)$ and $C_\Omega(D, G)$, respectively, if it is clear which curve is meant. See Goppa [5], [6], [7], [8], [9], or [16], or [22].

Theorem 1 .
a) If $m < n$ then $C_L(D, G)$ is a linear $[n, k, d]$ code with

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

If moreover $2g - 2 < m$ then $k = m + 1 - g$.
b) If $2g - 2 < m$ then $C_\Omega(D, G)$ is a linear $[n, k, d]$ code with

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

If moreover $m < n$ then $k = n - m - 1 + g$.

Proof: See [5], [16] or [22].

Proposition 1 *The linear code $C_\Omega(D, G)$ is the dual of $C_L(D, G)$.*

Proof: See [8], [16] or [22].

Definition 2 We call a q-ary linear code C *weakly algebraic-geometric* (WAG) if there exists a projective, nonsingular, absolutely irreducible curve $\mathcal{X}$ defined over $\mathbf{F}_q$ of genus g, and n distinct rational points $P_1, \ldots, P_n$ on $\mathcal{X}$ and a divisor G with support disjoint from the support of D, where $D = P_1 + \ldots + P_n$, such that $C = C_L(\mathcal{X}, D, G)$. We call the triple $(\mathcal{X}, D, G)$ a *weakly algebraic-geometric representation* (WAG representation), or shortly, a *representation* of C. An *algebraic-geometric representation* (AG representation) is a representation $(\mathcal{X}, D, G)$ with $\deg(G) < n$. We call a code *algebraic-geometric* (AG) if it has an AG representation. A *strongly algebraic-geometric representation* (SAG representation) is a representation $(\mathcal{X}, D, G)$ with $2g - 2 < \deg(G) < n$. A code is called *strongly algebraic-geometric* (SAG) if it has a SAG representation.

Remark 1 There exists a differential form ω with a simple pole at each P_i and such that $res_{P_i}(\omega) = 1$ for $i = 1, \ldots, n$. We have $C_\Omega(\mathcal{X}, D, G) = C_L(\mathcal{X}, D, (\omega) - G + D)$, see [21, Corollary 2.6] or [16, Lemma 3.5]. As a consequence we have that C is WAG if and only if $C = C_\Omega(\mathcal{X}, D, G)$ for some curve $\mathcal{X}$ and divisors D and G as above (without the constraints on the degree of G). The code C is AG if moreover $2g - 2 < \deg(G)$. The code C is SAG if moreover $2g - 2 < \deg(G) < n$. In view of Proposition 1 we therefore have the following corollary.

Corollary 1 *If C is WAG or SAG, then $C^\perp$ is WAG, SAG, respectively.*

Remark 2 There exist codes which are AG while the dual is not. For an example, see Remark 13.

Definition 3 Let $n > 1$. Let $\pi_i : \mathbf{F}_q^n \to \mathbf{F}_q^{n-1}$ be the projection defined by deleting the i^{th} coordinate. If C is a code in $\mathbf{F}_q^n$ then define C_i by $C_i = \pi_i(C)$. We say that C_i is obtained from C by *puncturing* at the i^{th} coordinate.

Lemma 1 *If C is WAG then C_i is WAG.*

Proof: Suppose that $C = C_L(\mathcal{X}, D, G)$, where $D = (P_1, \ldots, P_n)$.
Let $D_i = (P_1, \ldots, P_{i-1}, P_{i+1}, \ldots, P_n)$. Then $C_i = C_L(\mathcal{X}, D_i, G)$.

Remark 3 If C is AG or SAG, then C_i need not be AG, SAG ,respectively, see Remark 19.

Definition 4 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 $\lambda = (\lambda_1, \ldots, \lambda_n)$ be an n-tuple of non zero elements in $\mathbf{F}_q$. Define

$$\lambda C = \{(\lambda_1 x_1, \ldots, \lambda_n x_n) | (x_1, \ldots, x_n) \in C\}.$$

The codes C_1 and C_2 are called *generalized equivalent* or *isometric* if there is an n-tuple $\lambda = (\lambda_1, \ldots, \lambda_n)$ of nonzero elements in $\mathbf{F}_q$ and a permutation σ such that $C_2 = \lambda\sigma C_1$.

Lemma 2 *If C_1 and C_2 are isometric codes and C_1 is WAG, AG or SAG, then C_2 is WAG, AG, SAG, respectively.*

Proof: Suppose $C_1 = C_L(\mathcal{X}, D, G)$ and $C_2 = \lambda\sigma C_1$ for some non zero elements $\lambda_1, \ldots, \lambda_n$ in $\mathbf{F}_q$ and a permutation σ. There exists a rational function f such that $f(P_{\sigma(i)}) = \lambda_i$ for all i, by the independence of valuations, see [2, p.11]. Let $\sigma D = (P_{\sigma(1)}, \ldots, P_{\sigma(n)})$. Then the divisor $G - (f)$ has disjoint support with σD, since all the λ_i are nonzero. We have $C_2 = C_L(\mathcal{X}, \sigma D, G - (f))$ and C_2 is WAG. The degrees of G and $G - (f)$ are equal. So, if C_1 is AG or SAG, then C_2 is AG, SAG, respectively.

Definition 5 We call a q-ary linear $[n, k]$ code *projective* if every two columns of a generator matrix of C are linearly independent. Thus if we view the columns of a generator matrix as points in the $(k-1)$-dimensional projective space $\mathbf{P}^{k-1}$, expressed in homogeneous coordinates, then we get n distinct points. This definition is obviously independent from the generator matrix chosen. By $S(r, q)$ we denote any q-ary projective code of dimension r and length $(q^r - 1)/(q - 1)$. Such a code is called a *Simplex* code. By $H(r, q)$ we denote the dual of $S(r, q)$. This is a q-ary *Hamming* code of redundancy r. If all the n points of a projective code lie in the complement of a hyperplane then we call the code *affine*.

Remark 4 If $n \geq 3$, then a code C is projective if and only if $d(C^\perp) \geq 3$. The code C is affine if and only if C is projective and there exists a codeword with weight equal to the word length. The maximal word length of a projective code of dimension r is $(q^r - 1)/(q - 1)$. For fixed r and q all q-ary Simplex codes of dimension r are isometric. The same holds for Hamming codes. The maximal possible word length of an affine code of dimension r is q^{r-1}. For fixed q and r all affine q-ary codes of dimension r and word

length q^{r-1} are isometric and are called *q-ary first order Reed-Muller* codes.

Remark 5 Suppose C is an affine code and we want to show that it is WAG. By Lemma 2, we may assume after an isometry, that the all one vector is a code word and it is the first row of a generator matrix of C. Let the n points $Q_1, \ldots, Q_n$ in $\mathbf{P}^{k-1}$ correspond to the n columns of the generator matrix. Suppose there exists an absolutely irreducible, projective curve $\mathcal{X}$ over $\mathbf{F}_q$ in $\mathbf{P}^{k-1}$, which goes through $Q_1, \ldots, Q_n$. The curve may be singular, but suppose there exists a rational point P_i in $n^{-1}(Q_i)$, for every i, where $n : \tilde{\mathcal{X}} \to \mathcal{X}$ is the normalization. Let $x_0, \ldots, x_{k-1}$ be homogeneous coordinates of $\mathbf{P}^{k-1}$ corresponding to the first upto the k^{th} row of the generator matrix. Then none of the points $Q_1, \ldots, Q_n$ lies in the hyperplane H, given by $x_0 = 0$. Let $G = n^*(\mathcal{X} \cdot H)$ be the pull back of the intersection divisor $\mathcal{X} \cdot H$ to the normalization. Let $f_i = (x_i/x_0) \circ n$. Then $f_0, \ldots, f_{k-1} \in L(G)$ and they are linearly independent, since the rank of the generator matrix of C is k. So $l(G) \geq k$. If $l(G) = k$ then $C = C_L(\tilde{\mathcal{X}}, D, G)$, where $D = (P_1, \ldots, P_n)$, that is to say C is WAG. In other words, we are looking for a curve $\mathcal{X}$ in $\mathbf{P}^{k-1}$ going through $Q_1, \ldots, Q_n$ such that the linear system of hyperplane sections of $\mathcal{X}$ is complete, and such that for every i there is a rational point in $n^{-1}(Q_i)$. In the next section we show that indeed there exists such a curve, going through all the q^{k-1} rational points of $\mathbf{P}^{k-1}$ outside a hyperplane. Such curves were called *covering* curves by Goppa [9, Ch.4,Sect.10]. Goppa [7, p.78] claimed that every linear code is WAG. In the proof he only mentioned that if $Q_1, \ldots, Q_n$ are n distinct points in $\mathbf{P}^{k-1}$, then there exists a curve passing through $Q_1, \ldots, Q_n$. First of all this reasoning only applies to *projective* codes, and secondly, the linear system of hyperplane sections of this curve does not need to be *complete*. This would only prove that every projective code is a subcode of a WAG code, see Lachaud [14, (5.10)].

Remark 6 Let C be a q-ary projective code of dimension at least 2. Suppose $C = C_L(\mathcal{X}, D, G)$ for some curve $\mathcal{X}$ and divisors D and G. If $L(G) = L(G - P)$ for some point P of $\mathcal{X}$, then P is not in the support of D. Otherwise $P = P_i$ for some $i \in \{1, \ldots, n\}$, so all the codewords have a zero at place i, contradicting the assumption that C is projective. Thus $G - P$ has disjoint support with D and $C = C_L(\mathcal{X}, D, G - P)$. Repeating this procedure we may assume without loss of generality that G is a divisor such that $L(G) \neq L(G - P)$ for all points P, that is to say G has no base points. Let $lG) = l$ and let $f_0, \ldots, f_{l-1}$ be a basis of $L(G)$. Consider the morphism

$$\varphi_G : \mathcal{X} \to \mathbf{P}^{l-1},$$

given by the collection of morphisms $\{\varphi_j : \mathcal{X} \backslash \mathrm{supp}(G_j) \to \mathbf{P}^{l-1}\}_{j=0}^{l-1}$, where $G_j = G + (f_j)$, and φ_j is defined by

$$\varphi_j(P) = (\frac{f_0}{f_j}(P) : \ldots : \frac{f_{l-1}}{f_j}(P)),$$

for $P \in \mathcal{X} \setminus \mathrm{supp}(G_j)$, see [12, p.128]. Then $\varphi_G(P) = (f_0(P) : \ldots : f_{l-1}(P))$, for $P \in \mathcal{X} \backslash \mathrm{supp}(G)$. This holds in particular for the P_i. The morphism φ_G depends only on the linear equivalence class of G, and on the choice of the basis $f_0, \ldots, f_{l-1}$ of $L(G)$. A different

choice of a basis of $L(G)$ gives a morphism which differs by an automorphism of $\mathbf{P}^{l-1}$ (see [11, p.158]). Let $\mathcal{X}_0$ be the reduced image of $\mathcal{X}$ under the morphism φ_G. Then $\mathcal{X}_0$ is not a single point. Even stronger, $\mathcal{X}_0$ is not contained in any hyperplane. This follows from the fact that $f_0, f_1, \ldots, f_{l-1}$ are linearly independent. Hence φ_G is a finite dominant morphism $\mathcal{X} \to \mathcal{X}_0$ of curves. Since $\mathcal{X}$ is absolutely irreducible, $\mathcal{X}_0$ is absolutely irreducible too. Finally, we have

$$\deg(G) = \deg(\varphi_G) \cdot \deg(\mathcal{X}_0),$$

since G has no base points, see [12, p.213] .

Definition 6 Let C be a projective code of dimension at least 2. If $(\mathcal{X}, D, G)$ is a (WAG, AG or SAG) representation of C and G is a divisor without base points and $\deg(\varphi_G) = 1$, then we call $(\mathcal{X}, D, G)$ a *minimal* (WAG, AG or SAG) representation of C (respectively).

Proposition 2 *Suppose C is a projective WAG code of dimension at least two. If $(\mathcal{X}, D, G)$ is a representation of C, with G base point free, then there exists a minimal representation $(\tilde{\mathcal{X}}_0, \tilde{D}, \tilde{G})$ of C and a finite morphism $\varphi : \mathcal{X} \to \tilde{\mathcal{X}}_0$ with the following properties:*
i) $\tilde{D} = (\varphi(P_1), \ldots, \varphi(P_n))$.
ii) $\varphi^*(\tilde{G}) \sim G$, where $\varphi^*(\tilde{G})$ is the pull back of $\tilde{G}$ under φ.
iii) $deg(\varphi) = deg(\varphi_G)$.
iv) $deg(\tilde{G}) = deg(G)/deg(\varphi) \leq deg(G)$.
v) $g(\tilde{\mathcal{X}}_0) \leq g(\mathcal{X})$, with equality if and only if $deg(\varphi) = 1$.
vi) If $(\mathcal{X}, D, G)$ is an AG representation, then so is $(\tilde{\mathcal{X}}_0, \tilde{D}, \tilde{G})$.
vi) If $(\mathcal{X}, D, G)$ is a SAG representation, then so is $(\tilde{\mathcal{X}}_0, \tilde{D}, \tilde{G})$.

Proof: Let $l(G) = l$. The kernel of the linear map α_L is $L(G-D)$, see Definition 1. We have $k = \dim(C) = l(G) - l(G-D)$. Let $f_0, \ldots, f_{l-1}$ be a basis of $L(G)$ such that $f_k, \ldots, f_{l-1}$ is a basis of $L(G-D)$. Let A be the $(l \times n)$- matrix

$$(f_j(P_i))_{j=0,\ldots,l-1;i=1,\ldots,n}.$$

The first k rows of A form a generator matrix of C. The remaining $l-k$ rows have only zero entries. Let the morphism φ_G be defined by the above basis of $L(G)$. The reduced image $\mathcal{X}_0$ of $\mathcal{X}$ under φ_G is possibly singular. Let $n : \tilde{\mathcal{X}}_0 \to \mathcal{X}_0$ be the normalization of $\mathcal{X}_0$. Then n is a birational morphism. Hence we have a rational map $\tilde{\varphi}_G : \mathcal{X} \to \tilde{\mathcal{X}}_0$ such that $n \circ \tilde{\varphi}_G = \varphi_G$. The curve $\mathcal{X}$ is nonsingular, hence $\tilde{\varphi}_G$ is a morphism. The n points $\tilde{\varphi}_G(P_i)$ $(i = 1, \ldots, n)$ are rational and we claim that they are all distinct. Indeed, if $\tilde{\varphi}_G(P_s) = \tilde{\varphi}_G(P_t)$ then $\varphi_G(P_s) = \varphi_G(P_t)$. But $\varphi_G(P_s)$ corresponds to the s^{th} column of the matrix A, and C is projective, hence $s = t$. Put $\tilde{P}_i = \tilde{\varphi}_G(P_i)$ and $\tilde{D} = (\tilde{P}_1, \ldots, \tilde{P}_n)$. For $j = 0, \ldots, l-1$, we denote by g_j the function x_j/x_0, which is a rational function on $\mathcal{X}_0$ such that $f_j/f_0 = g_j \circ \varphi_G$. We denote $g_j \circ n$ by $\tilde{g}_j$. Let H be the hyperplane in $\mathbf{P}^{l-1}$ with equation $x_0 = 0$ and let $H \cdot \mathcal{X}_0$ be the intersection divisor of H with $\mathcal{X}_0$. Define $G_0 := G + (f_0)$. The pull back $\varphi_G^*(H \cdot \mathcal{X}_0)$ is equal to G_0. Let $\tilde{G}_0 = n^*(H \cdot \mathcal{X}_0)$. Then $\tilde{\varphi}_G$ induces an injective map $\tilde{\varphi}_G^*$ from the function

field of $\tilde{\mathcal{X}}_0$ into the function field of $\mathcal{X}$, and maps $L(\tilde{G}_0)$ injectively into $L(G_0)$. This map is also surjective since $\tilde{\varphi}_G^*(\tilde{g}_j) = f_j/f_0$, for $j = 0, \ldots, l-1$, and $1, f_1/f_0, \ldots, f_{l-1}/f_0$ is a basis of $L(G_0)$. Let $\varphi_{\tilde{G}_0}$ be defined by the basis $\tilde{g}_0, \ldots, \tilde{g}_{l-1}$ of $L(\tilde{G}_0)$. Note that $\varphi_{\tilde{G}_0}$ is equal to the normalization map n. There exists a divisor $\tilde{G}$ which is linearly equivalent with $\tilde{G}_0$ and has disjoint support with $\tilde{D}$, by the theorem of independence of valuations, see [2, p.11]. We have $\varphi_{\tilde{G}} = \varphi_{\tilde{G}_0}$, where $\varphi_{\tilde{G}}$ is defined by a suitable choice of a basis of $L(\tilde{G})$. Hence $\varphi_{\tilde{G}}(\tilde{P}_i) = n \circ \tilde{\varphi}_G(P_i) = \varphi_G(P_i)$, for $i = 1, \ldots, n$. All these points have their last $l-k$ coordinates equal to zero. Thus there is an n-tuple $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbf{F}_q^n$, with all $\lambda_i \neq 0$, such that $C_L(\tilde{\mathcal{X}}_0, \tilde{D}, \tilde{G}) = \lambda C_L(\mathcal{X}, D, G)$. As we see from the proof of Lemma 2, we may assume without loss of generality that $C_L(\tilde{\mathcal{X}}_0, \tilde{D}, \tilde{G}) = C_L(\mathcal{X}, D, G)$. In the proposition choose $\varphi = \tilde{\varphi}_G$. We have $\deg(\varphi_{\tilde{G}}) = \deg(n) = 1$, $\deg(\varphi) = \deg(\varphi_G)$ and

$$\deg(\tilde{G}) = \deg(\tilde{G}_0) = \frac{\deg(G_0)}{\deg(\varphi)} = \frac{\deg(G)}{\deg(\varphi_G)} \leq \deg(G),$$

see the end of Remark 6. Since G is base point free and φ^* restricts to an isomorphism $L(\tilde{G}_0) \to L(G_0)$, $\tilde{G}$ is base point free too. Since φ^* preserves linear equivalence and $\tilde{G} \sim \tilde{G}_0$, we have $\varphi^*(\tilde{G}) \sim \varphi^*(\tilde{G}_0) = G_0 \sim G$. This proves everything in the proposition, except *v),vi)* and *vii)*. Note that *vi)* is an immediate consequence of *iv)*. Part *v)* and part *vii)* will follow by the genus formula of Zeuthen-Hurwitz, see [16, p.52] or [11, p.301]. First we prove that φ is separable. The morphism $\varphi : \mathcal{X} \to \tilde{\mathcal{X}}_0$ factorizes into $\varphi = \varphi_s \circ \varphi_i$, where

$$\varphi_i : \mathcal{X} \to \mathcal{X}_i$$

is purely inseparable and

$$\varphi_s : \mathcal{X}_i \to \tilde{\mathcal{X}}_0$$

is separable, see [11, p.303,Example 2.5.4]. The morphism φ_i induces an inclusion

$$\varphi_i^* : \mathbf{F}_q(\mathcal{X}_i) \hookrightarrow \mathbf{F}_q(\mathcal{X}),$$

and the image is equal to

$$\{f^{p^r} | f \in \mathbf{F}_q(\mathcal{X})\} = \mathbf{F}_q(\mathcal{X})^{p^r},$$

where $p^r = \deg(\varphi_i)$, p is the charactaristic of $\mathbf{F}_q$ and r is some nonnegative integer. The curve $\mathcal{X}_i$ is isomorphic with $\mathcal{X}$, see [11, p.302,Prop.2.5]. Let

$$\psi : \mathcal{X}_i \to \mathcal{X}$$

be the isomorphism (of curves) which induces the isomorphism (of function fields)

$$\psi^* : \mathbf{F}_q(\mathcal{X}) \to \mathbf{F}_q(\mathcal{X}_i), f \mapsto f^{p^r}.$$

Put $G_i := \varphi_s^*(\tilde{G}_0)$. Define the divisor G_i' on $\mathcal{X}$ by $\psi^*(G_i') = G_i$. Then $G_0 = \varphi^*(\tilde{G}_0) = \varphi_i^*(\varphi_s^*(\tilde{G}_0)) = \varphi_i^*(G_i) = p^r G_i'$. The map φ_i^* maps $L(G_i)$ injectively into $L(G_0)$. The morphism φ_s induces an inclusion

$$\varphi_s^* : \mathbf{F}_q(\tilde{\mathcal{X}}_0) \hookrightarrow \mathbf{F}_q(\mathcal{X}_i),$$

and φ_s^* maps $L(\tilde{G}_0)$ injectively into $L(G_i)$. Thus $l(\tilde{G}_0) \leq l(G_i) \leq l(G_0)$. But, as we saw earlier in the proof of this proposition, $l(G_0) = l(\tilde{G}_0)$, hence

$$l(G_i) = l(G_0). \tag{1}$$

Now suppose that $\deg(\varphi_i) > 1$, that is to say $r > 0$. Let $P \in \mathrm{supp}(G_i')$. Then

$$G_i' \leq (p^r - 1)G_i' \leq p^r G_i' - P = G_0 - P \leq G_0.$$

Hence

$$L(G_i') \subseteq L(G_0 - P) \subseteq L(G_0). \tag{2}$$

On the other hand, ψ^* restricts to an isomorphism $L(G_i) \to L(G_i')$, hence $l(G_i) = l(G_i')$, and by (1), $l(G_0) = l(G_i')$. This implies that the inclusions in (2) are equalities, and hence that P is a basepoint of G_0, a contradiction. Thus $\deg(\varphi_i) = 1$, and φ is separable. So we can apply the genus formula of Zeuthen-Hurwitz to φ:

$$2g(\mathcal{X}) - 2 = (2g(\tilde{\mathcal{X}}_0) - 2)\deg(\varphi) + \deg(R),$$

where R is the ramification divisor of φ, which is effective. As shown in [11, p.303,Example 2.5.4], it follows that $g(\mathcal{X}) \geq g(\tilde{\mathcal{X}}_0)$. Note that if $\deg(\varphi) = 1$, then $R = 0$. One easily verifies that $g(\mathcal{X}) = g(\tilde{\mathcal{X}}_0)$ if and only if

$$\deg(\varphi) = 1,$$

or

$$g(\mathcal{X}) = 0,$$

or

$$g(\mathcal{X}) = 1 \text{ with } \varphi \text{ unramified.}$$

However, in our situation, the second and the third case are included in the first. Namely, suppose that $g(\mathcal{X}) = g(\tilde{\mathcal{X}}_0) =: g \leq 1$. We have $2 \leq k \leq l(G) = l(\tilde{G}_0)$, hence $\deg(G) > 0 \geq 2g - 2$ and $\deg(\tilde{G}_0) > 0 \geq 2g - 2$, and by Riemann-Roch

$$l(G_0) = \deg(G) + 1 - g,$$

$$l(\tilde{G}_0) = \deg(\tilde{G}_0) + 1 - g.$$

Since $l(G_0) = l(\tilde{G}_0)$, we get $\deg(G_0) = \deg(\tilde{G}_0) = \deg(G_0)/\deg(\varphi)$, hence $\deg(\varphi) = 1$. This proves *v)*. Finally, if $\deg(G) > 2g(\mathcal{X}) - 2$, then

$$\deg(\tilde{G}) = \frac{\deg(G)}{\deg(\varphi)} > \frac{2g(\mathcal{X}) - 2}{\deg(\varphi)} \geq 2g(\tilde{\mathcal{X}}_0) - 2.$$

This proves *vii)* and completes the proof of the proposition.

Corollary 2 *Suppose that $(\mathcal{X}, D, G)$ is a WAG representation of a projective code C of dimension at least two, with G base point free, and such that $g(\mathcal{X})$ is minimal, that is to say, for all WAG representations $(\mathcal{X}', D', G')$ of C we have $g(\mathcal{X}) \leq g(\mathcal{X}')$. Then $(\mathcal{X}, D, G)$ is a minimal WAG representation of C. This corollary is also true if 'WAG' is replaced by 'AG' everywhere, or by 'SAG'.*

Proof: Let $(\tilde{\mathcal{X}}_0, \tilde{D}, \tilde{G})$ be a minimal WAG representation of C with the properties as in Proposition 2. By the assumption on $g(\mathcal{X})$, and by Prop. 2*(v)*, we have $g(\tilde{\mathcal{X}}_0) = g(\mathcal{X})$, and hence $\deg(\varphi_G) = \deg(\varphi) = 1$, by Prop. 2*(iii)*. Since G is base point free, moreover, $(\mathcal{X}, D, G)$ is minimal. The two assertions in the second part of the corollary are proved similarly, using Prop. 2*(vi)* and 2*(vii)*, respectively.

III. All linear codes are weakly algebraic-geometric

Remark 7 Hansen and Stichtenoth [10] considered the curve $\mathcal{X}$ in $\mathbf{P}^2$ defined by the homogeneous equation

$$x^{q_0}(x^q + xz^{q-1}) = z^{q_0}(y^q + yz^{q-1}),$$

where $q_0 = 2^n$ and $q = 2^{2n+1}$. This curve is absolutely irreducible, has exactly one (singular) point P_∞ at the line $z = 0$, and goes through all the rational points outside the line $z = 0$. The linear system of hyperplane sections of this curve is complete. Inspired by their result we consider the following series of curves.

Definition 7 Let p be a prime number and q a power of p. Let $\mathcal{X}(l, q)$ be the closed subscheme over $\mathbf{F}_p$ in $\mathbf{P}^l$ defined by the homogeneous ideal

$$I(l, q) = (x_i^{q+1} - x_i^2 x_0^{q-1} + x_{i+1} x_0^q - x_{i+1}^q x_0, i = 1, \ldots, l-1)$$

in $\mathbf{F}_p[x_0, \ldots, x_l]$.

Proposition 3 *The scheme $\mathcal{X}(l, q)$ is a projective, absolutely irreducible, reduced curve over $\mathbf{F}_p$. It has exactly one point P_∞ at the hyperplane H with equation $x_0 = 0$, the curve is nonsingular outside P_∞ and goes through all the q^l rational points of $\mathbf{P}^l$ outside the hyperplane H.*

Proof: The scheme $\mathcal{X}(l, q)$ is defined by $l-1$ equations, hence all the irreducible components are at least one dimensional. $P_\infty = (0 : \ldots : 0 : 1)$ is the only point in the intersection with H, which follows directly from the equations. Let

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

Then $f_1 = \ldots = f_{l-1} = 0$ are the equations of $\mathcal{X}(l, q)$ on the complement of H, which is isomorphic with affine l-space with coordinates $y_1, \ldots, y_l$, where $y_i = x_i/x_0$. For every fixed

y_1 there are exactly q^{l-1} solutions $\mathbf{y} = (y_1, \ldots, y_l)$ in $\mathbf{F}_q^l$ as well as in $\bar{\mathbf{F}}_q^l$ of the equations $f_1, \ldots, f_{l-1} = 0$. Hence $\mathcal{X}(l,q)$ has dimension one and is a complete intersection. Let $f = (f_1, \ldots, f_{l-1})$. Computing the derivative of f gives

$$df = \begin{pmatrix} y_1^q - 2y_1 & 1 & & 0 \\ & \ddots & \ddots & \\ 0 & & y_{l-1}^q - 2y_{l-1} & 1 \end{pmatrix}$$

Hence df has maximal rank at all points not equal to P_∞ of $\mathcal{X}(l,q)$ over $\bar{\mathbf{F}}_q$. Thus the curve is nonsingular outside P_∞. Thus $\mathcal{X}(l,q)$ is reduced outside P_∞ and a complete intersection, and therefore it is reduced. Let

$$n : \tilde{\mathcal{X}}(l,q) \longrightarrow \mathcal{X}(l,q)$$

be the normalization of $\mathcal{X}(l,q)$ and $\tilde{P}_\infty$ any point in $n^{-1}(P_\infty)$. Let v_∞ be the discrete valuation at $\tilde{P}_\infty$. Let $z_i = y_i \circ n$. Then $z_1, \ldots, z_l$ are rational functions on $\tilde{\mathcal{X}}(l,q)$ and have no poles outside $n^{-1}(P_\infty)$. Furthermore

$$z_i^{q+1} - z_i^2 = z_{i+1}^q - z_{i+1}$$

Thus

$$(q+1)v_\infty(z_i) = qv_\infty(z_{i+1})$$

Now z_1 has a pole at $\tilde{P}_\infty$, hence $v_\infty(z_1)$ is negative. Hence by induction one shows that there exists a positive integer a such that

$$v_\infty(z_i) = -aq^{l-i}(q+1)^{i-1}.$$

Consider the map $\varphi : \mathcal{X}(l,q) \to \mathcal{Y}$, which is the projection with center the subspace with equations $x_0 = x_1 = 0$, of the curve in $\mathbf{P}^l$ onto the line $\mathcal{Y}$ defined by the equations $x_2 = \ldots = x_l = 0$. Then $t = x_0/x_1$ is a local parameter of the point $Q_\infty = (0:1:0:\ldots:0)$ in $\mathcal{Y}$. Let the map $\tilde{\varphi} : \tilde{\mathcal{X}}(l,q) \to \mathcal{Y}$ be defined by $\tilde{\varphi} = \varphi \circ n$. Then $\tilde{P}_\infty$ is a point of $\tilde{\varphi}^{-1}(Q_\infty)$ and $v_\infty(t) = aq^{l-1}$, so the ramification index $e_{\tilde{P}_\infty}$ of $\tilde{\varphi}$ at $\tilde{P}_\infty$ is at least q^{l-1}. For every other point Q of $\mathcal{Y}(\bar{\mathbf{F}}_q)$ not equal to Q_∞, the inverse image $\tilde{\varphi}^{-1}(Q)$ consists of exactly q^{l-1} points over $\bar{\mathbf{F}}_q$, all with ramification index one, since the map

$$d\tilde{\varphi} : T_{\tilde{Q}}(\tilde{\mathcal{X}}(l,q)) \longrightarrow T_Q(\mathcal{Y})$$

between the tangent spaces, is surjective, as one sees from the derivative df of f. Thus $\deg(\tilde{\varphi}) = q^{l-1} \leq e_{\tilde{P}_\infty}$. Therefore $\tilde{\mathcal{X}}(l,q)$ is absolutely irreducible and $n^{-1}(P_\infty) = \{\tilde{P}_\infty\}$, by the following lemma, and thus $\mathcal{X}(l,q)$ is absolutely irreducible. This proves the proposition.

Lemma 3 *Let $\mathcal{X}$ and $\mathcal{Y}$ be projective, nonsingular curves over an algebraically closed field. Suppose $\mathcal{Y}$ is irreducible. Let $\varphi : \mathcal{X} \to \mathcal{Y}$ be a finite morphism. Suppose there exist points P_∞ in $\mathcal{X}$ and Q_∞ in $\mathcal{Y}$ such that $\varphi(P_\infty) = Q_\infty$ and the ramification index e_{P_∞} of φ at P_∞ is at least $deg(\varphi)$. Then $deg(\varphi) = e_{P_\infty}$ and $\mathcal{X}$ is irreducible and $\{P_\infty\} = \varphi^{-1}(Q_\infty)$.*

Proof: Suppose $\mathcal{X}_1, \ldots, \mathcal{X}_s$ are the irreducible components of $\mathcal{X}$. Let φ_i be the restriction of φ to $\mathcal{X}_i$. Then

$$\deg(\varphi) = \sum_{i=1}^{s} \deg(\varphi_i) = \sum_{P \in \varphi^{-1}(Q)} e_P,$$

for every point Q of $\mathcal{Y}$. Suppose $P_\infty \in \mathcal{X}_1$. Then

$$\deg(\varphi) \geq \deg(\varphi_1) \geq e_{P_\infty} \geq \deg(\varphi).$$

Thus $\deg(\varphi) = \deg(\varphi_1) = e_{P\infty}$. So $\{P_\infty\} = \varphi^{-1}(Q_\infty)$ and $\mathcal{X}_1$ is the only irreducible component of $\mathcal{X}$, that is to say $\mathcal{X}$ is irreducible. This proves the lemma.

Proposition 4 *The normalization of $\mathcal{X}(l,q)$ has genus $g(l,q)$, where*

$$g(l,q) = \frac{1}{2}\{\sum_{i=1}^{l-1} q^{l+1-i}(q+1)^{i-1} - (q+1)^{l-1} + 1\}$$

Proof: It follows from the proof of Proposition 3 that

$$v_\infty(z_i) = -q^{l-i}(q+1)^{i-1}$$

and $n^{-1}(P_\infty)$ consists of exactly one point $\tilde{P}_\infty$. Let

$$u = \prod_{i=1}^{l} z_i \begin{pmatrix} l-1 \\ i-1 \end{pmatrix}^{(-1)^{l-1-i}}$$

Then u is a local parameter of $\tilde{P}_\infty$, since

$$\begin{aligned} v_\infty(u) &= \textstyle\sum_{i=1}^{l} \begin{pmatrix} l-1 \\ i-1 \end{pmatrix} (-1)^{l-1-i} v_\infty(z_i) \\ &= \textstyle\sum_{i=0}^{l-1} \begin{pmatrix} l-1 \\ i \end{pmatrix} (-q)^{l-1-i}(q+1)^i \\ &= [-q+(q+1)]^{l-1} = 1 \end{aligned}$$

Differentiating the equation

$$z_{i+1} - z_{i+1}^q = z_i^{q+1} - z_i^2 \quad \text{for} \quad 1 \leq i \leq l-1,$$

with respect to z_i gives

$$\frac{dz_{i+1}}{dz_i} = 2z_i - z_i^q.$$

Hence we get by the chain rule and induction

$$\frac{dz_j}{dz_1} = \prod_{i=1}^{j-1}(2z_i - z_i^q).$$

Let $t = z_1^{-1}$. Then t is a local parameter of Q_∞ in $\mathcal{Y}$. Thus

$$\frac{du}{dt} = -z_1^2 \frac{du}{dz_1}$$

$$= -z_1^2 \{ \sum_{i=1}^{l} \prod_{j \neq i} z_j \binom{l-1}{j-1}^{(-1)^{l-1-j}} \binom{l-1}{i-1} (-1)^{l-1-i} z_i \binom{l-1}{i-1}^{(-1)^{l-1-i}-1} \frac{dz_i}{dz_1} \}$$

$$= -z_1^2 \{ \sum_{i=1}^{l} \binom{l-1}{i-1} (-1)^{l-1-i} u z_i^{-1} \frac{dz_i}{dz_1} \}.$$

Now

$$v_\infty(z_i^{-1} \frac{dz_i}{dz_1}) = q^{l-i}(q+1)^{i-1} - \sum_{j=1}^{i-1} q q^{l-j}(q+1)^{j-1} > v_\infty(z_{i+1}^{-1} \frac{dz_{i+1}}{dz_1}).$$

Therefore

$$v_\infty(\frac{du}{dt}) = v_\infty(z_1^2 u z_l^{-1} \frac{dz_l}{dz_1}).$$

And we conclude

$$v_\infty(\frac{dt}{du}) = \sum_{i=1}^{l-1} q^{l+1-i}(q+1)^{i-1} + 2q^{l-1} - 1 - (q+1)^{l-1}.$$

The map $\tilde{\varphi}$ is separable, has degree q^{l-1} and is only ramified at $\tilde{P}_\infty$. Let $g = g(l,q)$. Then

$$2g - 2 = -2\deg(\tilde{\varphi}) + v_\infty(\frac{dt}{du}),$$

by the theorem of Hurwitz-Zeuthen, see [16]. Thus

$$g = \frac{1}{2} \{ \sum_{i=1}^{l-1} q^{l+1-i}(q+1)^{i-1} - (q+1)^{l-1} + 1 \}.$$

This proves the proposition.

Remark 8 Let P be a point on a nonsingular, absolutely irreducible curve $\mathcal{X}$ of genus g over a field. Let $N_n = dim(L(nP))$ for $n \in \mathbf{N}$. Then $1 = N_0 \leq N_1 \leq \ldots \leq N_{2g-1} = g$, so there are exactly g numbers $0 < n_1 < \ldots < n_g < 2g$, such that $L(n_i P) = L((n_i - 1)P)$. These n_i are called *Weierstrass gaps* of P. Furthermore, if $m \in \mathbf{N}$ then

$$N_n = \#\{m \in \mathbf{N} | m \leq n \text{ and } m \text{ is not a gap at } P\}.$$

See [4].

Definition 8 Let $\mathcal{G}(l,q) = \{n_1, n_2, \ldots n_g\}$ be the set of all gaps of $\tilde{P}_\infty$ on the curve

$\tilde{\mathcal{X}}(l,q)$ of genus $g = g(l,q)$.

Definition 9 Let

$$\mathcal{P}(l,q) = \{\sum_{i=1}^{l} k_i q^{l-i}(q+1)^{i-1} \mid k_i \in \mathbf{Z} \text{ and } k_i \geq 0\}.$$

Proposition 5

$$\mathcal{G}(l,q) = \mathbf{N} \setminus \mathcal{P}(l,q)$$

To prove this proposition we need the following lemmas.

Lemma 4 *For every $m \in \mathbf{Z}$, there are unique $u, v \in \mathbf{Z}$, such that*

$$m = uq + v(q+1)^{l-1} \quad \textit{and} \quad 0 \leq v < q.$$

Moreover, $m \in \mathcal{P}(l,q)$ if and only if $u \in \mathcal{P}(l-1,q)$.

Proof: Since

$$1 = -\{\sum_{i=1}^{l-1} \left(\begin{array}{c} l-1 \\ i \end{array} \right) q^{i-1}\}q + (q+1)^{l-1},$$

we have that

$$m = -m\{\sum_{i=1}^{l-1} \left(\begin{array}{c} l-1 \\ i \end{array} \right) q^{i-1}\}q + m(q+1)^{l-1},$$

for every $m \in \mathbf{N}$, furthermore there exist $a, b \in \mathbf{N}$ such that $m = aq + b$ and $0 \leq b < q$, so

$$m = \{a(q+1)^{l-1} - m\sum_{i=1}^{l-1} \left(\begin{array}{c} l-1 \\ i \end{array} \right) q^{i-1}\}q + b(q+1)^{l-1}.$$

Let

$$u = a(q+1)^{l-1} - m\sum_{i=1}^{l-1} \left(\begin{array}{c} l-1 \\ i \end{array} \right) q^{i-1} \quad \text{and} \quad v = b,$$

then $m = uq + v(q+1)^{l-1}$ and $0 \leq v < q$. If there are another $u_1, v_1 \in \mathbf{Z}$, such that $m = u_1 q + v_1(q+1)^{l-1}$ and $0 \leq v_1 < q$ then we can assume without loss of generality that $u_1 \geq u$, thus $(u_1 - u)q + (v_1 - v)(q+1)^{l-1} = 0$, so q divides $(v_1 - v)$, so $v_1 = v$, and $u_1 = u$ as well. Therefore such u and v are unique.
Now suppose $m = uq + v(q+1)^{l-1}$ and $0 \leq v < q$.
If $m \in \mathcal{P}(l,q)$, then $m = \sum_{i=1}^{l} k_i q^{l-i}(q+1)^{i-1}$ where k_i is a non negative integer for $i = 1, \ldots, l$. But $k_l = aq + b$,where $a, b \in \mathbf{N}$ and $0 \leq b < q$,so

$$m = \{\sum_{i=1}^{l-1} k_i q^{l-1-i}(q+1)^{i-1} + a(q+1)(q+1)^{l-2}\}q + b(q+1)^{l-1},$$

hence $u = \sum_{i=1}^{l-1} j_i q^{l-1-i}(q+1)^{i-1}$, by the uniqueness of u, where $j_i = k_i$ for $i = 1, \ldots, l-2$ and $j_{l-1} = k_{l-1} + a(q+1)$. Thus $u \in \mathcal{P}(l-1, q)$.
If $u \in \mathcal{P}(l-1, q)$ then $u = \sum_{i=1}^{l-1} j_i q^{l-1-i}(q+1)^{i-1}$ for some non negative integers $j_1, \ldots, j_{l-1}$ so

$$m = \{\sum_{i=1}^{l-1} j_i q^{l-1-i}(q+1)^{i-1}\}q + v(q+1)^{l-1} \in \mathcal{P}(l, q).$$

This proves the lemma.

Lemma 5

$$\#(\mathbf{N} \setminus \mathcal{P}(l, q)) = g(l, q)$$

Proof: By induction on l.
(i) We have that $\mathcal{P}(2, q) = \{iq + j(q+1) \mid i, j \in \mathbf{N}\}$, so

$$\mathbf{N} \setminus \mathcal{P}(2, q) = \bigcup_{k=0}^{q-2} \{kq + (k+1), kq + (k+1) + 1, \ldots, (k+1)q - 1\},$$

which is a union of mutually disjoint sets, hence

$$\#(\mathbf{N} \setminus \mathcal{P}(2, q)) = (q-1) + (q-2) + \ldots + 2 + 1 = \frac{1}{2}q(q-1),$$

which satisfies the conclusion.
(ii) Assume the conlusion is true for $l-1$. By Lemma 4 we have that

$$\mathbf{N} = \{uq + v(q-1)^{l-1} \mid u < 0, 0 \leq v < q\} \cup \{uq + v(q+1)^{l-1} \mid u \geq 0, 0 \leq v < q\},$$

where the two sets are disjoint . We denote the first set by $\mathbf{N}_1$, and the second one by $\mathbf{N}_2$. Then

$$\mathbf{N} \setminus \mathcal{P}(l, q) = (\mathbf{N}_1 \setminus \mathcal{P}(l, q)) \cup (\mathbf{N}_2 \setminus \mathcal{P}(l, q)).$$

1) For each $uq + v(q-1)^{l-1} \in \mathbf{N}_2 \setminus \mathcal{P}(l, q)$, we have $u \in \mathbf{N} \setminus \mathcal{P}(l-1, q)$ by Lemma 4, so

$$\#(\mathbf{N}_2 \setminus \mathcal{P}(l, q)) = q\#(\mathbf{N} \setminus \mathcal{P}(l-1, q)) = \frac{1}{2}q\{\sum_{j=1}^{l-2} q^{l-j}(q+1)^{j-1} - (q+1)^{l-2} + 1\}.$$

2) For each $uq + v(q-1)^{l-1} \in \mathbf{N}_1 \setminus \mathcal{P}(l, q)$, we have $u < 0$ and $0 \leq v < q$. Hence

$$uq + v(q+1)^{l-1} \geq 1 \Leftrightarrow -uq \leq v(q+1)^{l-1} - 1$$

$$\Leftrightarrow -uq \leq v\{\sum_{i=1}^{l-1} \begin{pmatrix} l-1 \\ i \end{pmatrix} q^i\} + v - 1$$

$$\Leftrightarrow -u \leq v \sum_{i=1}^{l-1} \begin{pmatrix} l-1 \\ i \end{pmatrix} q^{i-1},$$

since $v-1<q-1$. Hence

$$\#(\mathbf{N}_1 \setminus \mathcal{P}(l,q)) = \sum_{v=1}^{q-1} v \sum_{i=1}^{l-1} \left(\begin{array}{c} l-1 \\ i \end{array} \right) q^{i-1}$$

$$= \frac{1}{2}q(q-1)\sum_{i=1}^{l-1} \left(\begin{array}{c} l-1 \\ i \end{array} \right) q^{i-1} = \frac{1}{2}\{q(q+1)^{l-1} - (q+1)^{l-1} - q + 1\}.$$

Combining 1) and 2) gives

$$\#(\mathbf{N} \setminus \mathcal{P}(l,q)) = \frac{1}{2}\{\sum_{i=1}^{l-2} q^{l+1-i}(q+1)^{i-1} - q(q+1)^{l-2} + q +$$

$$+q(q+1)^{l-1} - (q+1)^{l-1} - q + 1\}$$

$$= \frac{1}{2}\{\sum_{i=1}^{l-1} q^{l+1-i}(q+1)^{i-1} - (q+1)^{l-1} + 1\} = g(l,q).$$

This proves the lemma.

Proof of Proposition 5: If $m \in \mathcal{P}(l,q)$ then $m = \sum_{i=1}^{l} k_i q^{l-i}(q+1)^i$, where k_i is a non negative integer for $i = 1, \ldots, l$. Now

$$v_\infty(z_1^{k_1} z_2^{k_2} \ldots z_l^{k_l}) = -\sum_{i=1}^{l} k_i q^{l-i}(q+1)^i = -m,$$

since $v_\infty(z_i) = -q^{l-i}(q+1)^{i-1}$ for $i = 1, \ldots, l$. So $z_1^{k_1} z_2^{k_2} \ldots z_l^{k_l}$ is an element of $L(m\tilde{P}_\infty)$ and not of $L((m-1)\tilde{P}_\infty)$, hence m is not a gap of $\tilde{P}_\infty$, so $\mathcal{G}(l,q) \subseteq \mathbf{N}\backslash\mathcal{P}(l,q)$. But by Lemma 5 we have that $\#\mathcal{G}(l,q) = g(l,q) = \#(\mathbf{N}\backslash\mathcal{P}(l,q))$. Therefore $\mathcal{G}(l,q) = \mathbf{N}\backslash\mathcal{P}(l,q)$. This proves the proposition.

Proposition 6 *The vector space $L(m\tilde{P}_\infty)$ is generated by*

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

Proof: This follows from Proposition 5 and Remark 8.

Corollary 3 *If $2q^{l-1} > q^{l-i}(q+1)^{i-1}$ then $1, z_1, \ldots, z_i$ is a basis of $L(q^{l-i}(q+1)^{i-1}\tilde{P}_\infty)$.*

Proof: It follows from Proposition 6 and the assumption that $1, z_1, \ldots, z_i$ generate the vector space we consider. The valuations at P_∞ of these $i+1$ elements are mutually distinct, so they are independent.

Corollary 4 *A q-ary first order Reed-Muller code of dimension 3 is AG.*

Proof: A q-ary first order Reed-Muller code of dimension 3 is represented by $(\mathcal{X}(2,q), D, G)$, by Corollary 3, where $P_1, \ldots, P_{q^2}$ are the q^2 rational points of the complement in $\mathbf{P}^2$ of the line with equation $x_0 = 0$, and $D = \sum_{i=1}^{q^2} P_i$ and $G = (q+1)\tilde{P}_\infty$. The divisor G has degree $q+1$ which is smaller than q^2. This proves the corollary.

Proposition 7 *If C is a q-ary linear code which has a code word of weight equal to the word length, then C is WAG.*

Proof: Let C have dimension k. We may assume that the all one vector is a code word, by Lemma 2. Choose a generator matrix of C such that the all one vector is the first row. Let $Q_1, \ldots, Q_n$ be the points of $\mathbf{P}^{k-1}$ corresponding to the n columns of the generator matrix. Define

$$s = max\{t| \text{ there exist } i_1 < \ldots < i_t \text{ such that } Q_{i_1} = \ldots = Q_{i_t}\}.$$

Let $l = [k + log_q s]$. Then $s \leq q^{l-k+1}$ and there are n distinct points $P_1, \ldots, P_n$, rational over $\mathbf{F}_q$, in $\mathbf{P}^l$ such that $\pi(P_i) = Q_i$, where $\pi : \mathbf{P}^l \setminus H \to \mathbf{P}^{k-1}$ is defined by $\pi(x_0 : \ldots : x_l) = (x_0 : \ldots : x_{k-1})$ and H is the hyperplane with equation $x_0 = 0$, since the fibres of π are isomorphic with $\mathbf{A}^{l-k+1}$. Choose a power q_0 of q such that $2q_0^{l-1} > q_0^{l-k}(q_0+1)^{k-1}$. Let $\mathcal{X} = \tilde{\mathcal{X}}(l, q_0)$ and $G = q_0^{l-k}(q_0+1)^{k-1}\tilde{P}_\infty$ and $D = P_1 + \ldots + P_n$. Then $C = C_L(\mathcal{X}, D, G)$ by Corollary 3 and C is WAG. This proves the proposition.

Theorem 2 *Every linear code is WAG.*

Proof: Let C be a linear code. Then the dual of the extended code $\overline{C}$ of C, has word length $n+1$ and the all one vector is an element of $(\overline{C})^\perp$. Thus $(\overline{C})^\perp$ is WAG by Proposition 7, so $\overline{C}$ is WAG by Corollary 1. But C can be obtained from $\overline{C}$ by puncturing at the last coordinate. Therefore C is WAG, by Lemma 1. This proves the theorem.

IV. Criteria for linear codes to be algebraic-geometric

We first mention a few well-known theorems (Theorems 3,4,5) and bounds on the genus of a curve.

Definition 10 For any divisor D on a nonsingular, absolutely irreducible curve $\mathcal{X}$ over a field we define $l(D) = \dim L(D)$ and $i(D) = \dim \Omega(D)$.

Remark 9 If $\deg(D) < 0$ then $l(D) = 0$. If $\deg(D) > 2g - 2$ then $i(D) = 0$, where g is the genus of the curve. The Riemann-Roch Theorem states that

$$l(D) = \deg(D) + 1 - g + i(D).$$

So it gives a lower bound on $l(D)$ in terms of the degree of D. The following theorem gives an upper bound.

Theorem 3 (Clifford) *If $l(D) > 0$ and $i(D) > 0$, then $l(D) \leq \frac{1}{2}deg(D) + 1$.*

Proof: See [11].

Remark 10 A *hyperelliptic* curve is an absolutely irreducible, nonsingular curve of genus at least two, which has a morphism of degree two to the projective line. The pull back under this morphism of a point of degree one on the projective line is called a *hyperelliptic* divisor. A hyperelliptic curve over $\mathbf{F}_q$ has at most 2q+2 rational points. If $g \geq 2$, then we have equality in Clifford's theorem if and only if D is a principal or a canonical divisor or the curve is hyperelliptic and the divisor D is linearly equivalent with a multiple of a hyperelliptic divisor, see [11, p.343].

Definition 11 Let $N_q(g)$ be the maximal number of rational points on a nonsingular, absolutely irreducible curve, over $\mathbf{F}_q$ of genus g.

Theorem 4 (Serre's bound)

$$N_q(g) \leq q + 1 + g[2\sqrt{q}].$$

Furthermore,

$$N_2(g) \leq 0.83g + 5.35,$$

Proof: See [20].

Remark 11 Table I gives some exactly determined values of $N_q(g)$. See [16, p.34],[19] and [20].

Table I. Some known values of $N_q(g)$.

g	0	1	2	3	4	5	6	7	8	9	15	19	21	39	50
$N_2(g)$	3	5	6	7	8	9	10	10	11	12	17	20	21	33	40
$N_3(g)$	4	7	8	10											
$N_4(g)$	5	9	10	14											

Theorem 5 (Castelnuovo's bound) . *Let $l \geq 1$. If $\mathcal{X}$ is an absolutely irreducible curve, over $\mathbf{F}_q$, in $\mathbf{P}^l$ and not contained in any hyperplane, then*

$$g(\mathcal{X}) \leq \pi(m, l).$$

Here m is the degree of $\mathcal{X}$ in $\mathbf{P}^l$, and $\pi(m, l)$ is defined by

$$\pi(m, 1) = 0,$$

$$\pi(m,l) = \frac{t(t-1)}{2}(l-1) + t\varepsilon, \ \textit{if } l > 1,$$

where t is an integer such that $m-1 = t(l-1)+\varepsilon$ and $0 \leq \varepsilon < l-1$.

Proof: See [1], where the proof is given for curves over the complex numbers. In [11] the proof is given in arbitrary characteristic for $l = 3$. One can easily make a proof for arbitrary l and in any characteristic, by a combination of [1] and [11].

Remark 12 It is easily verified that $\pi(m,l) \leq \pi(m',l)$, if $m \leq m'$.

The following proposition is hidden in a remark of Katsman and Tsfasman, see [13].

Proposition 8 *Let C be an $[n,k]$ code. If C is AG, then $2k \leq n+d^\perp-1$, where $d^\perp = d^\perp(C)$ is the minimum distance of $C^\perp$.*

Proof: If $C^\perp$ is MDS then $d^\perp = k+1$, hence $2k \leq n+d^\perp-1$. So we may assume that $C^\perp$ is not MDS, that is to say $d^\perp \leq k$. If C is an AG code, then $C = C_L(D,G)$ for some divisor G of degree $m < n$ and $k = l(G)$. Now $C^\perp = C_\Omega(D,G)$, so there exist $d^\perp$ distinct indices $i_1, \ldots, i_{d^\perp}$ and a differential $\omega \in \Omega(G-D)$, such that $res_{P_{i_j}}(\omega) \neq 0$ for $j = 1 \ldots d^\perp$, and $res_{P_i}(\omega) = 0$ for $i \notin \{i_1, \ldots, i_{d^\perp}\}$. Put $D_1 = \sum_{j=1}^{d^\perp} P_{i_j}$. Then ω is an element of $\Omega(G-D_1)$ and not of $\Omega(G)$. But $\Omega(G-D_1)$ contains $\Omega(G)$, so

$$i(G-D_1) \geq i(G)+1 > 0.$$

Hence

$$l(G-D_1) = m - d^\perp + 1 - g + i(G-D_1) \geq$$
$$\geq m+1-g+i(G)-d^\perp+1 = k-d^\perp+1 > 0,$$

using the Riemann-Roch Theorem twice. We have

$$k-d^\perp+1 \leq l(G-D_1) \leq 1 + \frac{m-d^\perp}{2},$$

by Clifford's Theorem. Therefore $2k \leq m+d^\perp \leq n+d^\perp-1$, since $m \leq n-1$. This proves the proposition.

Remark 13 The q-ary first order Reed-Muller code C of dimension 3 has length q^2 and minimum distance $q(q-1)$, see [3]. By Corollary 4 this code is AG. If $q \geq 7$, then $C^\perp$ is not AG, by Proposition 8, since $2(q^2-3) > q^2+q(q-1)-1$ if $q \geq 7$. Thus we have examples of codes C such that C is AG and $C^\perp$ is not AG (see Remark 2).

Definition 12 let $g_q(n)$ be the minimal genus of a nonsingular, absolutely irreducible curve $\mathcal{X}$ over $\mathbf{F}_q$, with at least n rational points.

Remark 14 Serre's bound implies $n \leq q+1+g_q(n)[2\sqrt{q}]$, for all n

Proposition 9 *Suppose $(\mathcal{X}, D, G)$ is an AG representation of a q-ary $[n,k]$ code and let $m = deg(G)$ $(< n)$.*
a) If $m \leq 2g-2$, then $k \leq [(n+1)/2]$.
b) If $m > 2g-2$, then $g_q(n) \leq g \leq n-k$.

Proof: a) If $k = 0$, then there is nothing to prove. So assume $k > 0$, hence $l(G) = k > 0$. If $g \leq n-k$, then

$$k = l(G) = m + 1 - g + i(G) \leq g - 1 + i(G) \leq n - k - 1 + i(G),$$

hence $2k \leq n - 1 + i(G)$. It follows that $i(G) > 0$ or $k \leq (n-1)/2$.
If $g > n-k$, then

$$k = l(G) = m + 1 - g + i(G) < m + 1 - n + k + i(G) \leq k + i(G),$$

hence $i(G) > 0$.
If $i(G) > 0$, then $k = l(G) \leq m/2 + 1 \leq (n+1)/2$, by Clifford's Theorem. Thus in every case $k \leq [(n+1)/2]$.
b) If $m > 2g-2$, then $i(G) = 0$. Hence $k = m+1-g \leq n-g$. This proves the proposition.

Corollary 5 *There exists a q-ary $[n,k]$ SAG code if and only if*

$$g_q(n) \leq min\{k, n-k\}$$

Proof: If a q-ary $[n,k]$ code has a SAG representation, then $g_q(n) \leq n-k$, by Proposition 9b. The dual of this code is a SAG $[n, n-k]$ code, by Corollary 1. Hence, again by Proposition 9b, $g_q(n) \leq k$. Conversely, by definition, there exists a nonsingular, absolutely irreducible curve $\mathcal{X}$ over $\mathbf{F}_q$ of genus $g = g_q(n)$, having (at least) n distinct rational points, $P_1, \ldots, P_n$ say. Put $D = P_1 + \ldots + P_n$. There exists a divisor G of degree $k + g - 1$ and with disjoint support with D, by the theorem of independence of valuations. Now $2g - 2 < \deg(G) = k + g - 1 < n$, since $g \leq k$ and $g \leq n - k$. Thus $(\mathcal{X}, D, G)$ represents a SAG $[n,k]$ code. This proves the corollary.

Corollary 6 *If there exists a q-ary $[n,k]$ AG code, then*

$$k \leq [\frac{n+1}{2}] \quad if \quad g_q(n) > n-k$$

and

$$k \leq [\frac{([2\sqrt{q}]-1)n + q + 1}{[2\sqrt{q}]}] \quad if \quad g_q(n) \leq n-k.$$

Proof: Suppose $(\mathcal{X}, D, G)$ is an AG representation of a q-ary $[n,k]$ code. Let $m = \deg(G)$. If $g_q(n) > n-k$, then $m \leq 2g-2$, by Proposition 9b. Thus $k \leq [(n+1)/2]$, by Proposition 9a. If $g_q(n) \leq n-k$ then

$$n \leq q + 1 + g_q(n)[2\sqrt{q}] \leq q + 1 + (n-k)[2\sqrt{q}],$$

by Serre's bound, so

$$k \leq [\frac{([2\sqrt{q}]-1)n+q+1}{[2\sqrt{q}]}].$$

Remark 15 Here and in Section V we shall investigate which Hamming codes $H(r,q)$ are AG. The code $H(r,q)$ is only determined up to isometries (see Definition 5), but this question makes sense anyway, by Lemma 2.

Corollary 7 *If $r \geq 3$ and the Hamming code $H(r,q)$ is AG then $(r,q) = (3,2)$.*

Proof: Let $r \geq 3, n = (q^r-1)/(q-1)$ and $k = n-r$. Then $H(r,q)$ is an $[n,k]$ code, see Definition 5. The minimum distance of its dual is q^{r-1}. If $H(r,q)$ is AG then Proposition 8 implies that

$$2(\frac{q^r-1}{q-1} - r) \leq \frac{q^r-1}{q-1} + q^{r-1} - 1,$$

so

$$\frac{q^{r-1}-1}{q-1} < 2r.$$

This is only possible in case the pair (r,q) is equal to (3,2), (4,2), (3,3) or (3,4). To exclude the last three possibilities, observe that $g_2(15) > 4$, $g_3(13) > 3$ and $g_4(21) > 3$, by Table I, hence $g_q(n) > r = n-k$ in these three cases, and apply Corollary 6. Since in all three cases $k > [(n+1)/2]$, we get a contradiction. This proves the corollary.

Remark 16 In Section V we shall see that $H(1,q)$ and $H(2,q)$ are SAG, for every q, and that $H(3,2)$ is SAG.

Proposition 10 *Let $k \geq 2$. Let $(\mathcal{X}, D, G)$ be a minimal representation of a projective q-ary $[n,k]$ code. Let $l = l(G)$. Then*

$$g_q(n) \leq g(\mathcal{X}) \leq \pi(deg(G), l-1).$$

In particular, if $(\mathcal{X}, D, G)$ is AG, moreover, then

$$g_q(n) \leq g(\mathcal{X}) \leq \pi(deg(G), k-1).$$

Proof: By assumption, the divisor G has no base points and the morphism $\varphi_G : \mathcal{X} \to \mathbf{P}^{l-1}$ has degree one. Hence $\deg(\mathcal{X}_0) = \deg(G)$, where $\mathcal{X}_0$ is the reduced image of $\mathcal{X}$ under φ_G, see Remark 6. Since $\mathcal{X}$ has (at least) n rational points, we have $g_q(n) \leq g(\mathcal{X})$. Since $\deg(\varphi_G) = 1$, we have $g(\mathcal{X}) = g(\mathcal{X}_0)$. The result now follows from Castelnuovo's bound, applied to the curve $\mathcal{X}_0$, which is absolutely irreducible and does not lie in any hyperplane. The second part of the proposition follows from the fact that $\deg(G) < n$ implies $l = k$.

Corollary 8 *Let $k \geq 2$. If there exists a q-ary projective AG $[n,k]$ code then*

$$g_q(n) \leq \pi(n-1, k-1).$$

Proof: If a q-ary projective AG $[n,k]$ code exists, then there exists a minimal AG representation $(\tilde{\mathcal{X}}_0, \tilde{D}, \tilde{G})$ of this code, by Proposition 2. The result now follows from Proposition 10, applied to this minimal representation, and Remark 12, using $\deg(\tilde{G}) \leq n-1$.

Proposition 11 *If there exists a binary projective AG $[n,k]$ code, then*
a) If $n \geq 14$ or $n = 12$ then $k < [n/2]$,
b) If $n = 11$ or $n = 13$ then $k < n/2$.

Proof: If $k < [n/2]$, then there is nothing to prove. Suppose $k \geq [n/2]$. If $g_2(n) \leq n-k$ then

$$n \leq 0.83(n - [\frac{n}{2}]) + 5.35,$$

by Serre's bound, which implies $n < 10$. Suppose $n \geq 10$. Then $g_2(n) > n-k$, by the above. So by Corollary 6, we have

$$[\frac{n}{2}] \leq k \leq [\frac{n+1}{2}].$$

There are the following possibilities, a priori:
i) $k \geq 5$ and $n = 2k$,
ii) $k \geq 5$ and $n = 2k+1$,
iii) $k \geq 6$ and $n = 2k-1$.
In the first case $\pi(n-1, k-1) = k+2$. Hence $g_2(n) \leq k+2$, by Corollary 8. So $2k \leq 0.83(k+2) + 5.35$, by Serre's bound. Thus $k \leq 5$, and $n \leq 10$, and there is nothing to prove. Similarly we get $k \leq 6, n \leq 13$ in the second case, but now $k < n/2$. Finally, we get $k \leq 5, n \leq 9$ in the third case, which therefore cannot occur. Combining the above we get the desired result.

Corollary 9 *The binary Golay code and its extension are not AG.*

Proof: As we know, the minimal distances of the dual codes of the binary Golay code and its extension are greater than 3, see [17]. The binary Golay code is a [23,12] code and its extension a [24,12] code, so they are not AG, by Proposition 11.

Remark 17 Our results do not yield a similar result concerning the ternary Golay code and its extension. The question whether these codes are AG is still unanswered.

Corollary 10 *For every $t \geq 2$, $r \geq t$ and $\varepsilon \in \{0,1\}$, the r-th order binary Reed-Muller code $RM(r, 2t+\varepsilon)$ of length $2^{2t+\varepsilon}$ is not AG.*

Proof: Let $r > 1$ and $m = 2t+\varepsilon$, where $t \geq 2$ and $\varepsilon \in \{0,1\}$. The code $RM(m-r-1, m)$ is the dual code of $RM(r,m)$. The length of the codewords of $RM(r,m)$ is $n = 2^m$, the dimension of $RM(r,m)$ is $1 + \begin{pmatrix} m \\ 1 \end{pmatrix} + \ldots + \begin{pmatrix} m \\ r \end{pmatrix}$, and the minimum distance of $RM(r,m)$

is 2^{m-r}, see [3] and [17]. So $d^{\perp}(RM(r,m)) = 2^{r+1} > 3$. If $RM(r,m)$ is AG then, since $n \geq 16$,

$$\dim RM(r,m) \leq [\frac{n}{2}] - 1 = 2^{m-1} - 1,$$

by Proposition 11. However, if $m = 2t$ or $m = 2t+1$, and $r \geq t$, then

$$\dim RM(r,m) = 1 + \begin{pmatrix} m \\ 1 \end{pmatrix} + \ldots + \begin{pmatrix} m \\ r \end{pmatrix} \geq 2^{m-1} > 2^{m-1} - 1,$$

which gives a contradiction. This proves the proposition.

Lemma 6 . *Suppose $(\mathcal{X}, D, G)$ is an AG representation of an $[n,k]$ code. Then deg$(G) \leq k+g-1$. If $k \neq 0$ and deg$(G) < k+g-1$, then deg$(G) \geq 2k-2$.*

Proof: By the Riemann-Roch Theorem, $k = l(G) \geq \deg(G) - g + 1$, so $\deg(G) \leq k+g-1$. If $\deg(G) \neq k+g-1$, then by Clifford's Theorem $k \leq \frac{1}{2}\deg(G) + 1$, since $l(G) = k > 0$ and $i(G) = k - \deg(G) + g - 1 > 0$. Thus $\deg(G) \geq 2k-2$.

Corollary 11 . *If $(\mathcal{X}, D, G)$ is an AG representation of an $[n,k]$ code, and $g \leq n-k$ and $k > [n/2]$, then deg$(G) = k+g-1$.*

Proof: If $\deg(G) \neq k+g-1$ then $2k-2 \leq \deg(G) < k+g-1 \leq n-1$, by Lemma 6, so $k \leq [n/2]$. This contradicts the assumption on k.

Proposition 12 *(See Table II). Let C be a binary $[n,k]$ code with $4 \leq n \leq 10$. Let k_0 and k' be given by Table II.*
a) If $k > k_0$, then C is not AG.
b) Suppose that C is AG and projective, and that $k = k'$. Let $(\mathcal{X}, D, G)$ be a minimal AG representation of C. Let g be the genus of $\mathcal{X}$ and let $m =$deg(G). Then $(g,m) = (g',m')$ for one of the pairs (g',m') given in the last column.

Table II. Restrictions on binary AG $[n,k]$ codes,
see Proposition 12.

n	k_0	k'	(g',m')
10	5	5	$(6,9)$ $(7,9)$
9	5	5	$(5,8)$
8	4	4	$(4,6)$ $(4,7)$ $(5,7)$ $(6,7)$
7	4	4	$(3,6)$ $(4,6)$
6	4	4	$(2,5)$
		3	$(2,4)$ $(3,4)$ $(3,5)$ $(4,5)$ $(5,5)$ $(6,5)$
5	4	4	$(1,4)$
		3	$(1,3)$ $(2,4)$ $(3,4)$
4	3	3	$(1,3)$

Proof: a) For every n, the proof goes as follows. If $k > k_0$, then $k > [(n+1)/2]$, while $n - k < n - k_0 \leq g_2(n)$, by Table I. By Corollary 6, C cannot be AG.
b) We shall only give the proof for the case $n = 6$, $k = 3$. The proofs in the other cases are analogous, and sometimes simpler. So let $n = 6$ and $k = 3$. By Table I, $g_2(6) = 2$, hence $g \geq 2$. We have $m < n = 6$. If $m = 5$, then $2 \leq g \leq \pi(5, 2) = 6$, by Proposition 10. The case $(g, m) = (2, 5)$ is excluded by Lemma 6. If $m = 4$, then $2 \leq g \leq \pi(4, 2) = 3$, by Proposition 10. Since $\pi(3, 2) = 1 < 2 \leq g$, it is not possible that $m \leq 3$, by Proposition 10 and Remark 12.

Remark 18 In Proposition 12*b* we do *not* claim that for every pair (g', m') given in the table a minimal AG representation with $(g, m) = (g', m')$ actually exists. As a matter of fact, in the next section we shall prove that for $n = 7, k' = 4$, the case $(g', m') = (4, 6)$ is impossible!

Proposition 13 *There exists a binary SAG code of length n if and only if $n \leq 8$*

Proof: By Proposition 11, SAG codes of length $n \geq 11$ do not exist, since a SAG code is AG and its dual is too, but they cannot both have dimension $< n/2$. The cases with $n \leq 10$ are dealt with by Corollary 5 and Table I: only for $n \leq 8$ there exists a k such that $g_2(n) \leq \min\{k, n - k\}$.

Remark 19 (See Remark 3) There exists a binary SAG $[5, 4]$ code, by Corollary 5, since $g_2(5) = 1$, by Table I. This code is *a fortiori* AG. Puncturing this code gives a binary $[4, 4]$ code, which is not AG (and not SAG), by Proposition 12.

V. Explicit representations

In part A of this section we shall give a complete answer to the question: for which r and q is the Hamming code $H(r, q)$ AG? In the affirmative case we shall give an explicit AG representation, and discuss uniqueness. In part B of this section we shall discuss an example of a code which was mentioned in a different paper, and prove that it is SAG.

A. Hamming codes

Remark 20 Suppose that C is a linear code and that $(\mathcal{X}, D, G)$ is a representation of C, where $D = (P_1, \ldots, P_n)$. Now let G' be a divisor on $\mathcal{X}$ which is linearly equivalent with G, and which has disjoint support with D too. Let $C' = C_L(\mathcal{X}, D, G')$. Let f be a rational function on $\mathcal{X}$ such that $G = G' + (f)$. Then f is defined at P_i and $f(P_i) \neq 0$, for all i. In the special case (which is the only possible case if C is binary), that $f(P_i) = f(P_j)$ for

all i and j, we have $C = C'$. This is a sufficient, but, in general, not a necessary condition, by the way. By the theorem of independence of valuations, see [2, p.11], there are infinitely many rational functions f on $\mathcal{X}$ with $f(P_i) = 1$ for all i. Hence C has infinitely many representations $C_L(\mathcal{X}, D, G')$. Now return to the general case, where G' and f are arbitrary. Then $C' = \lambda C$, where $\lambda = (\lambda_1, \ldots, \lambda_n)$ and $\lambda_i = f(P_i) \in \mathbf{F}_q \setminus \{0\}$. If σ is a permutation of $\{1, \ldots, n\}$, then $C_L(\mathcal{X}, \sigma D, G) = \sigma C$. For the definition of λC, σC and σD, see Definition 4 and the proof of Lemma 2. We have $C_L(\mathcal{X}, \sigma D, G) = C$ if and only if $\sigma \in \mathrm{Aut}(C)$. Here $\mathrm{Aut}(C)$ is the automorphism group of C, see [17, p.229]. We see that the triple $(\mathcal{X}, \sigma D, G')$ represents a code that is isometric with C. The proof of Lemma 2 shows that every code isometric with C can be represented this way, that is to say, by a triple $(\mathcal{X}, \sigma D, G')$ for a suitable permutation σ and a divisor G' linearly equivalent with G. If $\mathcal{X}'$ is a curve and $\varphi : \mathcal{X}' \to \mathcal{X}$ is an isomorphism, then $C_L(\mathcal{X}', \varphi^*(D), \varphi^*(G))$ is also a representation of C. Here $\varphi^*(D)$ and $\varphi^*(G)$ denote the pull backs of D and G to $\mathcal{X}'$ under φ, respectively. When discussing uniqueness of representations of codes, one doesn't wish to distinguish between isomorphic curves, nor between linearly equivalent divisors G, nor between divisors D which can be obtained from each other by a permutation of the rational points in their support. By the above reasoning, it is therefore more convenient and more useful to think of a representation as a representation of the whole collection of codes isometric to a particular code, rather than to consider it as a representation of a *single* code. For given $\mathcal{X}$ and D it is actually sufficient only to specify the linear equivalence class of G, since in the linear equivalence class of any divisor there is a divisor which has disjoint support with D, by the independence of valuations.

Therefore, we introduce the following concepts.

Definition 13 *a)* If two linear codes C and C' are isometric, we denote this by $C \sim C'$. We define the *isometry class* of a linear code C to be the set of all codes which are isometric with C, and we denote this class by $[C]$.

b) Let $(\mathcal{X}, D, G)$ and $(\mathcal{X}', D', G')$ be representations (not necessarily of the same code). Let $D = (P_1, \ldots, P_n)$ and $D' = (Q_1, \ldots, Q_n)$. We call these representations *isometric*, denoted by $(\mathcal{X}, D, G) \sim (\mathcal{X}', D', G')$, if there exists an isomorphism $\varphi : \mathcal{X}' \to \mathcal{X}$ and a permutation σ of $\{1, \ldots, n\}$, such that $\varphi(Q_{\sigma(i)}) = P_i$, for all i, and such that the pull back $\varphi^*(G)$ of G is linearly equivalent with G'. We define the *isometry class* of a representation $(\mathcal{X}, D, G)$ to be the set of all representations isometric with this representation, and denote it by $[(\mathcal{X}, D, G)]$.

c) We call an isometry class $[(\mathcal{X}, D, G)]$ of representations a *representation class* of an isometry class $[C]$ of codes if $C_L(\mathcal{X}, D, G)$ is isometric with C.

Remark 21 *a)* Isometry of codes and isometry of representations are equivalence relations in the sets of codes and representations, respectively. The isometry classes defined in Definition 13*a)* and *b)* are the equivalence classes under these equivalence relations.

b) We call a representation class (WAG), AG, SAG or *minimal* according to whether there is a representation in this class which is (WAG), AG, SAG or minimal, respectively.

This definition is obviously independent from the choice of the representation. Besides, $\deg(G)$ and $g(\mathcal{X})$ do not depend on this choice either. Similarly, we can speak about a WAG, AG or SAG isometry class of codes, by Lemma 2.

c) As pointed out in Remark 20, isometric representations represent isometric codes, and if a code C is represented by $(\mathcal{X}, D, G)$, then for every code in $[C]$ there is a representation of this code in $[(\mathcal{X}, D, G)]$.

d) To specify a representation class it is of course sufficient only to give one of the representations in this class.

e) We shall not be too careful with the language we use to express that a (class of) code(s) is represented by a (class of) representation(s). But by Remark 20 there will never be misunderstandings about the right interpretation.

Remark 22 Recall from Section II (Definition 5 and Remark 4) that $H(r, q)$ denotes *any* q-ary linear code with parameters $[n = (q^r - 1)/(q - 1), n - r, 3]$ (codes of the same length and dimension, but with minimum distance greater than 3 do not exist). All such codes are isometric. From now on, we shall use the notation $H(r, q)$ also to denote the isometry class consisting of all the q-ary linear codes with these parameters. It is well-known and easily deduced from Definition 5 and Remark 4 that a q-ary linear code is a Simplex code $S(r, q)$ if and only if it has parameters $[n = (q^r - 1)/(q - 1), r, q^{r-1}]$. Similar to the case of the Hamming codes, we shall also use the notation $S(r, q)$ to denote the isometry class consisting of all the q-ary linear codes with these parameters.

In Section IV (Corollary 7) we already saw that the only Hamming codes that can possibly be AG are those with $r = 1$, $r = 2$, or $(r, q) = (3, 2)$. The cases $r = 1$ and $r = 2$ are dealt with by the following proposition.

Proposition 14 *For every q, $H(1, q)$ and $H(2, q)$ are SAG.*

Proof: Let $\mathcal{X} = \mathbf{P}^1$, the projective line over $\mathbf{F}_q$. Let $P_1, \ldots, P_{q+1}$ be the $\mathbf{F}_q$-rational points on $\mathcal{X}$. We have $H(1, q) = \{0\} = C_L(\mathcal{X}, D, G)$ if we choose $D = P_1$, $G = -P_2$. In this case $2g - 2 = -2 < -1 = deg(G) < 1 = n$. Hence $H(1, q)$ is SAG. To prove that $H(2, q)$ is SAG, take the same curve $\mathcal{X}$, but now take $D = P_1 + \cdots + P_{q+1}$, and let G be any divisor of degree $q - 2$, with support disjoint from the support of D. Since $g = 0$, $C_L(\mathcal{X}, D, G)$ is an MDS code with parameters $[n = q + 1,\ k = q - 2 + 1 = q - 1,\ d = q + 1 - (q - 2) = 3]$, by Theorem 1, i.e. $C_L(\mathcal{X}, D, G)$ is a Hamming code $H(2, q)$. We have $2g - 2 = -2 < q - 2 = deg(G) < q + 1 = n$. Hence $H(2, q)$ is SAG.

Remark 23 *a)* The number of SAG representation classes of a given code is always finite, because the genus g is upper bounded by $2g - 2 < m < n$, hence $g \leq n/2$, and because there are only finitely many nonisomorphic curves of a given genus, and the number h of linear equivalence classes of divisors of degree m is finite for each curve.

b) The number of *minimal* AG representation classes of a given projective code of dimension at least two is finite, since the genus g is upper bounded by $g \leq \pi(n - 1, k - 1)$, by Proposition 10 and Remark 12.

Remark 24 *a)* The SAG representation class of $H(1,q)$ given in the proof of Proposition 14 is *unique*, that is to say, $H(1,q)$ has no other SAG representation classes. Namely, suppose that $(\mathcal{X}, D, G)$ is a SAG representation of $H(1,q)$ and let $m = \deg(G)$. Then $2g-2 < m < n = 1$ implies $g = 0$ and $m \in \{-1, 0\}$. If $m = 0$, then the dimension of $C_L(\mathcal{X}, D, G)$ is one. Hence $m = -1$. All divisors of degree -1 on $\mathcal{X}$ are linearly equivalent.

b) There are infinitely many AG representation classes of $H(1,q)$. Namely, choose any curve $\mathcal{X}$ over $\mathbf{F}_q$ having at least one rational point, P_1 say. Put $D = P_1$. Let G be any divisor on $\mathcal{X}$ with $P_1 \notin \mathrm{supp}(G)$ and $\deg(G) < 0$. Then $L(G) = \{0\}$ and $C_L(\mathcal{X}, D, G)$ is an $H(1,q)$. We could also let G be a divisor of degree 0 on $\mathcal{X}$ which is not principal (such a G exists if and only if $h > 1$).

c) For example in the case $q = 2$ we find infinitely many AG representation classes of $H(2,q)$ as follows. Choose any curve $\mathcal{X}$ over $\mathbf{F}_2$ having at least three rational points, P_1,P_2 and P_3, say, and put $D = P_1 + P_2 + P_3$. Take $G = 0$. Then $L(G) = \{0, 1\}$, hence $C_L(\mathcal{X}, D, G) = \{000, 111\}$, which is an $H(2,2)$. If there is a fourth rational point on $\mathcal{X}$, P_4 say, then we could also take $G = P_4$ (and the same D). Namely, it follows that $g > 0$, and by Riemann-Roch and Clifford's theorem (see also [11, p.138,Example 6.10.1]), $l(G) = 1$, hence again $L(G) = \{0, 1\}$. If we choose for $\mathcal{X}$ an elliptic curve with at least four rational points, this latter example gives a representation which is not only AG, but even SAG, which shows that the SAG representation class of $H(2,q)$ given in the proof of Proposition 14 is *not* unique (at least for $q = 2$).

Let us now concentrate on $H(3,2)$. We shall prove that $H(3,2)$ is indeed AG (we shall even prove that it is SAG), and, moreover, that it has a *unique* minimal AG representation class. The latter statement is *not* true if we replace AG by WAG, as we shall see. To do so, let us first try to find a triple $(\mathcal{X}, D, G)$ such that the code $C_L(\mathcal{X}, D, G)$ is a binary code with parameters $[7, 4, 3]$, hence is equal to an $H(3,2)$. First of all, we need a nonsingular, absolutely irreducible projective curve defined over $\mathbf{F}_2$, having at least seven rational points. Such a curve cannot be hyperelliptic (since then it would have at most six rational points), and it has genus at least three (see Table I). If it has genus equal to three, such a curve, since not hyperelliptic, is isomorphic to a nonsingular and absolutely irreducible plane projective curve of degree four. Let S be the set consisting of all the (not necessarily nonsingular or absolutely irreducible, *a priori*) plane projective curves $\mathcal{X}$ of degree four, which have the following property: $\mathcal{X}$ goes through all the seven $\mathbf{F}_2$-rational points of $\mathbf{P}^2$, and none of these seven points is a singularity of $\mathcal{X}$. The set S is easily computed. It has 24 elements.

One of the curves in S is the following one, which we call $\mathcal{X}_1$, defined by

$$xy(x+y)(x+z) + xz^2(x+z) + y^2z(y+z) = 0. \tag{3}$$

This curve was mentioned earlier by Serre [20]. We have checked that $\mathcal{X}_1$ is nonsingular. By Bézout's theorem it is also absolutely irreducible. Let L be one of the seven lines defined over $\mathbf{F}_2$ in $\mathbf{P}^2$. By Bézout's theorem, the degree of the intersection divisor $L \cdot \mathcal{X}_1$ is 4. There are three rational points on L, which are also on $\mathcal{X}_1$. It follows that $\mathcal{X}_1$ intersects

L with multiplicity 2 at exactly one of them, and that the intersection is transversal at the two remaining points. In other words, the tangents to $\mathcal{X}_1$ at the seven rational points are precisely the seven lines defined over $\mathbf{F}_2$. We have named these points and lines, and computed the intersection divisors with the curve in Table III. We shall denote by L_i the tangent line to $\mathcal{X}_1$ at P_i, and by L_{ij} the line through P_i and P_j.

Table III. The $\mathbf{F}_2$-rational points P_i on the curve $\mathcal{X}_1$, the tangents L_i to $\mathcal{X}_1$ at these points, and the intersection divisors $L_i \cdot \mathcal{X}_1$.

P_i	L_i	$L_i \cdot \mathcal{X}_1$
$P_1 = (0:0:1)$	$x = 0$	$2P_1 + P_2 + P_3$
$P_2 = (0:1:0)$	$z = 0$	$2P_2 + P_4 + P_6$
$P_3 = (0:1:1)$	$y + z = 0$	$2P_3 + P_4 + P_7$
$P_4 = (1:0:0)$	$y = 0$	$P_1 + 2P_4 + P_5$
$P_5 = (1:0:1)$	$x + z = 0$	$P_2 + 2P_5 + P_7$
$P_6 = (1:1:0)$	$x + y + z = 0$	$P_3 + P_5 + 2P_6$
$P_7 = (1:1:1)$	$x + y = 0$	$P_1 + P_6 + 2P_7$

The group $PGL(2, \mathbf{F}_2)$ of $\mathbf{F}_2$-automorphisms of $\mathbf{P}^2$ acts on the set S, and has order 168. It also acts on the set $\{P_1, \ldots, P_7\}$ of $\mathbf{F}_2$-rational points, and on the set $\{L_1, \ldots, L_7\}$ of lines over $\mathbf{F}_2$. Put $\mathcal{H} := \{\tau \in PGL(2, \mathbf{F}_2) | \tau(P_1) = P_1\}$. This is a subgroup of $PGL(2, \mathbf{F}_2)$ of order 24.

Lemma 7 *$\mathcal{H}$ acts transitively on S.*

Proof: Suppose $\tau \in \mathcal{H}$ is such that $\tau\mathcal{X}_1 = \mathcal{X}_1$. Evidently, $\mathcal{H}$ acts on the group $\mathrm{Div}(\mathcal{X}_1)$ of divisors on $\mathcal{X}_1$, and for every i we have

$$\tau(L_i \cdot \mathcal{X}_1) = \tau L_i \cdot \tau\mathcal{X}_1 = \tau L_i \cdot \mathcal{X}_1 = L_j \cdot \mathcal{X}_1,$$

for some j. Since there is only one line L_i with $v_{P_1}(L_i \cdot \mathcal{X}_1) = 2$, L_1 namely, we must have $\tau L_1 = L_1$. Hence either *i)* $\tau(P_2) = P_2$ and $\tau(P_3) = P_3$, or *ii)* $\tau(P_2) = P_3$ and $\tau(P_3) = P_2$. For similar reasons, in case *i)*, $\tau L_2 = L_2$ and $\tau L_3 = L_3$, and in case *ii)* $\tau L_2 = L_3$ and $\tau L_3 = L_2$. In both cases we get $\{\tau(P_4)\} = \{\tau(L_2 \cap L_3)\} = \tau L_2 \cap \tau L_3 = L_2 \cap L_3 = \{P_4\}$. In case *i)* we now have three non-collinear points P_1, P_2, P_4 fixed by τ, which implies that τ is the identity. Case *ii)* cannot occur, because in this case it follows that $\tau(P_6) = P_7$ and $\tau(P_7) = P_6$, and we get $\tau(L_7 \cdot \mathcal{X}_1) = \tau(P_1 + P_6 + 2P_7) = P_1 + 2P_6 + P_7$, which is not an intersection divisor $L_j \cdot \mathcal{X}_1$, a contradiction. This proves that the $\mathcal{H}$-stabilizer of $\mathcal{X}_1$ is trivial, and hence that the $\mathcal{H}$-orbit of $\mathcal{X}_1$ has order 24. This proves the lemma.

By this lemma, all the 24 curves in the set S are isomorphic (even stronger: they only differ by a projective change of coordinates), and they are all nonsingular and absolutely irreducible, since $\mathcal{X}_1$ is. By the preceding discussion we have the following result.

Lemma 8 *Any absolutely irreducible nonsingular curve defined over* $\mathbf{F}_2$*, of genus three, having at least seven rational points, is isomorphic to the curve* $\mathcal{X}_1$*.*

So now we already have a curve $\mathcal{X}_1$ and a divisor $D_1 := P_1 + P_2 + \cdots + P_7$. The remaining problem is to find a suitable divisor G on $\mathcal{X}_1$, provided it exists.

Remark 25 The following lemma, does not only apply to our situation, but it is true for a general triple $(\mathcal{X}, D, G)$. It is an analogue of Lemma 6.

Lemma 9 *If* $(\mathcal{X}, D, G)$ *is a representation of a* q*-ary* $[n, k]$ *code and* $m :=$*deg*$(G) \geq n$*, then* $k = n$ *or* $k \geq (m + n)/2 - g$*.*

Proof: (See Definition 1). We have $k = l(G)-\dim(\text{kernel } \alpha_L)= l(G) - l(G - D) \leq n$, by the Riemann-Roch theorem. If inequality holds, then necessarily $\dim \Omega(G - D) > 0$, and by Clifford's theorem, $l(G - D) \leq 1 + (m - n)/2$. Hence $k = l(G) - l(G - D) \geq m + 1 - g - 1 - (m - n)/2 = (m + n)/2 - g$.

Returning to the specific curve $\mathcal{X}_1$, let $C := C_L(\mathcal{X}_1, D_1, G)$ have dimension k. If $k = 4$, then necessarily $\deg(G) = 6$ or $\deg(G) = 7$, by Lemmas 6 and 9. If $\deg(G) = 6$, then indeed $k = l(G) = 6 + 1 - 3 = 4$, by the Riemann-Roch theorem. If $\deg(G) = 7$, then $l(G) = 7 + 1 - 3 = 5$, and we have $k = l(G) - l(G - D_1)$, while $\deg(G - D_1) = 0$. Hence $k = 4$ in this case if and only if $G - D_1$ is a principal divisor, i.e. $G \sim D_1$. We have proved the following lemma.

Lemma 10 *The dimension of* $C = C_L(\mathcal{X}_1, D_1, G)$ *equals* 4 *if and only if* $deg(G) = 6$ *or* $G \sim D_1$ *(provided* $supp(G) \cap supp(D_1) = \emptyset$*).*

The thing left to do is to settle the problem that C might have the wrong minimum distance. Any binary [7,4] code has minimum distance at most 3, hence $d(C) \leq 3$.

The following lemma applies to the curve $\mathcal{X}_1$.

Lemma 11 *Let* $\mathcal{X}$ *be a non-hyperelliptic curve of genus* $g \geq 3$*. If* B *is an effective divisor on* $\mathcal{X}$ *of degree at most two, then* $l(B) = 1$*. Hence, if two effective divisors on* $\mathcal{X}$ *of degree at most two are equivalent, then they are equal.*

Proof: The case $B = 0$ is trivial. Suppose that $\deg(B) > 0$. Since B is effective, we have $1 \leq l(B) =\deg(B) + 1 - g + i(B)$, by the Riemann-Roch Theorem. Since $\deg(B) \leq 2$ and $g \geq 3$, it follows that $i(B) > 0$. Since $0 <\deg(B) < 4 \leq 2g - 2$, B is not principal or canonical, hence $l(B) < 1+\deg(B)/2 \leq 2$, by Clifford's Theorem, Remark 10, and the assumption that $\mathcal{X}$ is not hyperelliptic. This proves the lemma.

Proposition 15 *If* $G \sim D_1$ *(and* $supp(G) \cap supp(D_1) = \emptyset$*), then* $C = C_L(\mathcal{X}_1, D_1, G)$ *is a binary* $[7, 4, 3]$ *code.*

Proof: The only thing left to prove is that $d(C) \geq 3$. Let $G = D_1 + (f_0)$, with f_0 a nonzero rational function on $\mathcal{X}_1$. Since $\mathrm{supp}(G) \cap \mathrm{supp}(D_1) = \emptyset$, $v_{P_i}(f_0) = -1$ for $i = 1, 2, \ldots, 7$. A nonzero codeword of weight ≤ 2 exists if and only if an $f \in L(G) \backslash L(G - D_1)$ exists such that $(f) \geq -G + P_a + P_b + P_c + P_d + P_e$, for some distinct a, b, c, d, e. Since $G = D_1 + (f_0)$, this is equivalent to $(f) \geq -(f_0) - P_s - P_t$, for some distinct s and t, that is to say, $ff_0 \in L(P_s + P_t)$. But this cannot happen, since we would have $ff_0 = 1$, by Lemma 11, and hence $v_{P_i}(f) = -v_{P_i}(f_0) = 1$ for $i = 1, 2, \ldots, 7$, contradicting $f \notin L(G - D_1)$.

Remark 26 As already pointed out in Remark 20, divisors $G \in [D_1]$ with $\mathrm{supp}(G) \cap \mathrm{supp}(D_1) = \emptyset$ exist, by the theorem of independence of valuations. To give the representation explicitly, we need an explicit example of such a divisor. Let f_0 be the rational function on $\mathcal{X}_1$ defined as follows:

$$f_0 = \frac{H_2 H_3}{H_1 L_1 L_6},$$

where

$$H_1 = x^3z + x^2y^2 + x^2z^2 + xy^3 + y^3z + yz^3,$$
$$H_2 = x^3 + xy^2 + x^2z + xz^2 + y^2z + yz^2 + xyz,$$
$$H_3 = x^3 + y^3 + x^2y + xy^2 + xz^2 + yz^2 + xyz.$$

The equations of the lines L_1 and L_6 are $x = 0$ and $x + y + z = 0$, respectively, see Table III. For convenience, we use the same notation for a form and its zero set. Let Q be the place of degree 3 on $\mathcal{X}_1$ that corresponds to the orbit $\{(\alpha^2 : \alpha : 1), (\alpha^4 : \alpha^2 : 1), (\alpha : \alpha^4 : 1)\}$ of the $\mathbf{F}_8$-rational point $\{(\alpha^2 : \alpha : 1)\}$ on $\mathcal{X}_1$, where $Gal(\mathbf{F}_8/\mathbf{F}_2)$ is the group acting, and $\mathbf{F}_8 = \mathbf{F}_2(\alpha)$ with $\alpha^3 + \alpha + 1 = 0$. Let T and R be the places of degree 8 on $\mathcal{X}_1$ corresponding to the orbits of the $\mathbf{F}_{256}$-rational points $(\beta^6 : \beta^7 : 1)$ and $(\beta^{215} : \beta^{87} : 1)$ on $\mathcal{X}_1$, respectively, where $Gal(\mathbf{F}_{256}/\mathbf{F}_2)$ is the group acting, and $\mathbf{F}_{256} = \mathbf{F}_2(\beta)$ with $\beta^8 + \beta^4 + \beta^3 + \beta^2 + 1 = 0$. For the intersection divisors with the curve $\mathcal{X}_1$, we have

$$H_1 \cdot \mathcal{X}_1 = D_1 + 3Q,$$

$$H_2 \cdot \mathcal{X}_1 = P_1 + P_2 + P_3 + P_6 + T,$$
$$H_3 \cdot \mathcal{X}_1 = P_1 + P_3 + P_5 + P_6 + R,$$
$$L_1 \cdot \mathcal{X}_1 = 2P_1 + P_2 + P_3,$$
$$L_6 \cdot \mathcal{X}_1 = P_3 + P_5 + 2P_6.$$

The curve H_1 is one of the curves in the set S. Put $G_1 := D_1 + (f_0)$. Then

$$G_1 = T + R - 3Q.$$

We have $G_1 \sim D_1$ and $\mathrm{supp}(G_1) \cap \mathrm{supp}(D_1) = \emptyset$. Consequently, $(\mathcal{X}_1, D_1, G_1)$ is a WAG representation of an $H(3, 2)$.

This settles the case $G \sim D_1$. We shall now investigate the case $\deg(G) = 6$. This case requires more work. For $r := 1, 2, \ldots$, let N_r be the number of points (of degree one) on $\mathcal{X}_1$ over $\mathbf{F}_{2^r}$. Let $\mathcal{D}_i$ denote the set of all effective divisors on $\mathcal{X}_1$ of degree i, and let $a_i := \#\mathcal{D}_i$. One computes that $N_1 = 7$, $N_2 = 7$ and $N_3 = 10$. Hence there are no places of degree 2, and there is exactly one place of degree 3 on $\mathcal{X}_1$. This is the place Q mentioned in Remark 26. From N_1, N_2 and N_3 the zeta-function of $\mathcal{X}_1$ can be computed. The function $Z(\mathcal{X}_1, t)$, a rational function of t, is defined by

$$Z(\mathcal{X}_1, t) = \sum_{i=0}^{\infty} a_i t^i = \exp\left(\sum_{r=1}^{\infty} \frac{N_r}{r} t^r\right).$$

One computes that the polynomial

$$P(t) = 1 + 4t + 9t^2 + 15t^3 + 18t^4 + 16t^5 + 8t^6$$

satisfies

$$Z(\mathcal{X}_1, t) = \frac{P(t)}{(1-t)(1-2t)}.$$

It follows that

$$h = \#Pic_0(\mathcal{X}_1) = P(1) = 71,$$

and that

$$a_0 = 1,\ a_1 = 7,\ a_2 = 28,\ a_3 = 85.$$

For the underlying theory of zeta functions, see [16, p.66 a.f.], for instance.

Lemma 12 *Let B be a divisor of degree 3 on $\mathcal{X}_1$.*

a) If $B \sim P_a + P_b + P_c$ for three distinct collinear rational points P_a, P_b, P_c, then $l(B) = 2$. Otherwise, $l(B) = 1$.

b) Suppose B is effective, moreover. If $B \leq L_i \cdot \mathcal{X}_1$ for some i, then $l(B) = 2$. Otherwise $l(B) = 1$.

Proof: a) Consider the map $\phi : \mathcal{D}_3 \to Pic_3(\mathcal{X}_1)$, defined by $\phi(B) = [B]$, where $[B]$ is the linear equivalence class of B. Let B be a divisor on $\mathcal{X}_1$ of degree 3. By the Riemann-Roch theorem, $l(B) \geq 1$, and by Clifford's theorem, $l(B) \leq 2$. The number of inverse images of $[B]$ under ϕ equals $\#|B| = \#\mathbf{P}(L(B)) = 2^{l(B)} - 1$, which is 1 or 3. In particular, ϕ is surjective. Here $|B|$ is the complete linear system associated to B, that is the set of effective divisors linearly equivalent to B. Now suppose that a, b, c are distinct numbers such that P_a, P_b and P_c are collinear. Without loss of generality we may assume that the line through these three points is the line L_a. We can choose d, e, f, g such that $\{a, b, c, d, e, f, g\} = \{1, 2, \ldots, 7\}$ and

$$\begin{array}{rcccccc} L_a \cdot \mathcal{X}_1 & = & 2P_a & + & P_b & + & P_c, \\ L_d \cdot \mathcal{X}_1 & = & P_a & + & 2P_d & + & P_e, \\ L_f \cdot \mathcal{X}_1 & = & P_a & + & 2P_f & + & P_g. \end{array}$$

Now $0, 1, L_d/L_a, L_f/L_a$ are four distinct functions in $L(P_a + P_b + P_c)$. Hence $L(P_a + P_b + P_c) = \{0, 1, L_d/L_a, L_f/L_a\}$, $l(P_a + P_b + P_c) = 2$, and $\#|P_a + P_b + P_c| = 3$. We have

$$\left(\frac{L_d}{L_a}\right) = 2P_d + P_e - P_a - P_b - P_c,$$

$$\left(\frac{L_f}{L_a}\right) = 2P_f + P_g - P_a - P_b - P_c.$$

Hence $\phi^{-1}([P_a + P_b + P_c]) = |P_a + P_b + P_c| = \{P_a + P_b + P_c, 2P_d + P_e, 2P_f + P_g\}$. Since there are seven lines over $\mathbf{F}_2$ in $\mathbf{P}^2$, there are seven possibilities for $P_a + P_b + P_c$. These seven divisors represent seven *distinct* elements of $Pic_3(\mathcal{X}_1)$ (this follows from the above), each having three inverse images under ϕ. All the other $h - 7 = 71 - 7 = 64$ elements of $Pic_3(\mathcal{X}_1)$ must have exactly one inverse image, since $a_3 = 85 = 7 \cdot 3 + 64 \cdot 1$. So, for every divisor B not equivalent to one of the seven divisors $P_a + P_b + P_c$, we have $\#|B| = 1$, hence $l(B) = 1$. This proves *a)*.

b) This follows immediately from the proof of *a)*.

Lemma 13 *The group $PGL(2, \mathbf{F}_2)$ has an element τ of order 7 such that $\tau(\mathcal{X}_1) = \mathcal{X}_1$. For any such τ, the subgroup $< \tau >$ of $PGL(2, \mathbf{F}_2)$ generated by τ acts transitively on the set $\{P_1, P_2, \ldots, P_7\}$ of rational points.*

Proof: The automorphism $\tau\colon\ (x : y : z) \mapsto (x + y + z : x + y : y + z)$ has order 7. One easily verifies that $\tau(\mathcal{X}_1) = \mathcal{X}_1$. Let τ be an automorphism, not necessarily this one, of order 7 with $\tau(\mathcal{X}_1) = \mathcal{X}_1$. Then the $< \tau >$-orbit of P_1 has order 1 or 7. But, as we saw in the proof of Lemma 7, from $\tau(\mathcal{X}_1) = \mathcal{X}_1$ and $\tau(P_1) = P_1$, it would follow that τ is the identity, a contradiction. Hence the $< \tau >$-orbit of P_1 has order 7. This proves the lemma.

Proposition 16 *Suppose $deg(G) = 6$ (and $supp(G) \cap supp(D_1) = \emptyset$). Then $C = C_L(\mathcal{X}_1, D_1, G)$ is a binary $[7, 4, 3]$ code if and only if $G \sim 2Q$.*

Proof: A nonzero codeword of weight ≤ 2 corresponds to a $g_0 \in L(G)\backslash\{0\}$ with $(g_0) \geq -G + P_a + P_b + P_c + P_d + P_e$ for some distinct a, b, c, d, e. Since $\deg(-G + P_a + \cdots + P_e) = -1$, there is a rational point P_f such that $(g_0) = -G + P_a + \cdots + P_e + P_f$. Define the set of divisors Λ by

$$\Lambda := \{P_a + P_b + P_c + P_d + P_e + P_f | a, b, c, d, e \text{ distinct}\}$$

It follows that $d(C) = 3$ if and only if

$$G \not\sim E \text{ for all } E \in \Lambda. \tag{4}$$

The set Λ has 112 elements. Let us determine the number t of equivalence classes in Λ under the (induced) linear equivalence relation. For $E \in \Lambda$ we denote by $\overline{E}$ its equivalence class. Write

$$\Lambda = \Lambda^* \cup \Lambda_1 \cup \ldots \cup \Lambda_7,$$

(disjoint union), where

$$\Lambda^* = \{P_a + P_b + P_c + P_d + P_e + P_f | a, b, c, d, e, f \text{ distinct}\},$$

and

$$\Lambda_f = \{P_a + P_b + P_c + P_d + P_e + P_f | a, b, c, d, e \text{ distinct and } f \in \{a, b, c, d, e\}\}.$$

Then $\#\Lambda^* = 7$ and, for every f, $\#\Lambda_f = \begin{pmatrix} 6 \\ 4 \end{pmatrix} = 15$.

For every $E \in \Lambda^*$ we have $\#\overline{E} = 1$. Namely, if $E = P_a + P_b + \cdots + P_f \sim E'$ for an $E' = P_{a'} + P_{b'} + \cdots + P_{f'} \in \Lambda$, with a', b', c', d', e' distinct, then $\#(\{a, b, c, d, e, f\} \cap \{a', b', c', d', e'\}) \geq 4$. Without loss of generality $a = a'$, $b = b'$, $c = c'$, $d = d'$. Hence $P_e + P_f \sim P_{e'} + P_{f'}$. By Lemma 11, $P_e + P_f = P_{e'} + P_{f'}$, and hence $E = E'$.

For $f := 1, \ldots, 7$ and any i, define

$$w_i(f) := \#\{E \in \Lambda_f | \#\overline{E} = i\}.$$

We shall determine these numbers. By Lemma 13, $w_i(f) = w_i(1) =: w_i$, for all i and f, hence it suffices to consider the case $f = 1$. Suppose that $E = P_a + P_b + \cdots P_e + P_1 \in \Lambda_1$, $E' \in \Lambda$, $E \neq E'$ and $E \sim E'$. Then $E' \in \Lambda_{f'}$ for some f'. Write $E' = P_{a'} + P_{b'} + \cdots + P_{f'}$. Then $\#(\{a, b, c, d, e\} \cap \{a', b', c', d', e'\}) \geq 3$. Without loss of generality $c = c'$, $d = d'$, $e = e'$. Hence $P_a + P_b + P_1 \sim P_{a'} + P_{b'} + P_{f'}$. These two divisors are unequal, because E and E' are unequal. Hence $l(P_a + P_b + P_1) > 1$. Using Lemma 12 and Table III, one readily finds out that there are five possibilities for the divisor $P_a + P_b + P_1$. They are listed in the second column of Table IV. For each of them, following the proof of Lemma 12, one easily determines all the possible divisors $P_{a'} + P_{b'} + P_{f'}$. Except in the two cases $(P_a + P_b + P_1, P_{a'} + P_{b'} + P_{f'}) = (2P_1 + P_2, P_3 + P_4 + P_7)$ and $(P_a + P_b + P_1, P_{a'} + P_{b'} + P_{f'}) = (2P_1 + P_3, P_2 + P_4 + P_6)$, there is only one choice of f' and $\{c, d, e\}$, such that both a, b, c, d, e and a', b', c, d, e are five distinct numbers. In each of the two exceptional cases, there are three such choices.

Table IV. This table is used in the proof of Proposition 16.
All $E \in \Lambda_1$ with $\#\overline{E} > 1$ are listed.

$\{a,b\}$	$P_a+P_b+P_1$	$P_{a'}+P_{b'}+P_{f'}$	f'	$\{a',b'\}$	$\{c,d,e\}$	$E=$ $P_a+P_b+P_c+P_d+P_e+P_1$
$2,3$	$P_1+P_2+P_3$	$2P_4+P_5$	4	$4,5$	$1,6,7$	$2P_1+P_2+P_3+P_6+P_7$
		P_6+2P_7	7	$6,7$	$1,4,5$	$2P_1+P_2+P_3+P_4+P_5$
$4,5$	$P_1+P_4+P_5$	$2P_2+P_6$	2	$2,6$	$1,3,7$	$2P_1+P_3+P_4+P_5+P_7$
		$2P_3+P_7$	3	$3,7$	$1,2,6$	$2P_1+P_2+P_4+P_5+P_6$
$6,7$	$P_1+P_6+P_7$	$2P_3+P_4$	3	$3,4$	$1,2,5$	$2P_1+P_2+P_5+P_6+P_7$
		P_2+2P_5	5	$2,5$	$1,3,4$	$2P_1+P_3+P_4+P_6+P_7$
$1,2$	$2P_1+P_2$	$P_3+P_4+P_7$	3	$4,7$	$3,5,6$	$2P_1+P_2+P_3+P_5+P_6$
			4	$3,7$	$4,5,6$	$2P_1+P_2+P_4+P_5+P_6$
			7	$3,4$	$5,6,7$	$2P_1+P_2+P_5+P_6+P_7$
		P_5+2P_6	6	$5,6$	$3,4,7$	$2P_1+P_2+P_3+P_4+P_7$
$1,3$	$2P_1+P_3$	$P_2+P_4+P_6$	2	$4,6$	$2,5,7$	$2P_1+P_2+P_3+P_5+P_7$
			4	$2,6$	$4,5,7$	$2P_1+P_3+P_4+P_5+P_7$
			6	$2,4$	$5,6,7$	$2P_1+P_3+P_5+P_6+P_7$
		$2P_5+P_7$	5	$5,7$	$2,4,6$	$2P_1+P_2+P_3+P_4+P_6$

Of the fifteen elements of Λ_1, there are four which do not appear in the last column of Table IV, eight which appear once, and three which appear twice. Taking also the column with the values of f' into consideration, we see that $w_1=4$, $w_2=8$, and $w_3=3$, and that $w_i=0$ for $i>3$. Let t_i be the number of equivalence classes in Λ which have exactly i elements. We have

$$t_1=\#\Lambda^*+\sum_{f=1}^{7}w_1(f)=\#\Lambda^*+7w_1=7+7\cdot 4=35,$$

$$t_2=\frac{1}{2}\sum_{f=1}^{7}w_2(f)=7w_2/2=7\cdot 8/2=28,$$

$$t_3=\frac{1}{3}\sum_{f=1}^{7}w_3(f)=7w_3/3=7\cdot 3/3=7,$$

$$t_i=0 \text{ for } i>3.$$

Hence $t=\sum_i t_i=35+28+7=70$. But $h=\#Pic_6(\mathcal{X}_1)=71$. Hence there is a unique divisor G of degree 6 (up to linear equivalence) which satisfies (4). We claim that $2Q$ is such a divisor. To prove this, let τ be the automorphism mentioned at the beginning of the proof of Lemma 13. The group $<\tau>$ acts on the set $\mathrm{Div}(\mathcal{X}_1)$ of divisors on $\mathcal{X}_1$. Observe that $\tau Q=Q$, and that for any $E\in\Lambda$, the $<\tau>$-orbit of E is contained in Λ and has order 7. Now suppose that $2Q\sim E$, for some $E\in\Lambda$. Then $2Q=\tau^i 2Q\sim\tau^i E$, for all i. Hence the seven divisors in the $<\tau>$-orbit of E are equivalent elements in Λ. But we have

just seen that all equivalence classes in Λ have less than seven elements, a contradiction. This completes the proof of Proposition 16.

Remark 27 We find a basis of $L(2Q)$ and a generator matrix of $C_L(\mathcal{X}_1, D_1, 2Q)$ as follows. Define the forms

$$H_4 := x^2 + y^2 + z^2 + xy,$$
$$H_5 := y^2 + z^2 + xy + xz + yz$$

Then

$$H_4 \cdot \mathcal{X}_1 = P_3 + P_5 + 3P_7 + Q.$$
$$H_5 \cdot \mathcal{X}_1 = P_4 + 3P_5 + P_6 + Q,$$

Define the following rational functions on $\mathcal{X}_1$:

$$f_1 := \frac{H_5 L_1 L_3}{H_1},$$

$$f_2 := \frac{L_3 L_5 L_7^2}{H_4^2},$$

$$f_3 := \frac{L_4 L_5^2 L_6}{H_5^2},$$

The form H_1 was already defined in Remark 26. The lines L_3, L_5, L_7 and L_4, L_5, L_6 are the three lines through P_7 and P_5, respectively, see Table III. Now $\{1, f_1, f_2, f_3\}$ is a basis of $L(2Q)$. Indeed, we have

$$(1) = 0,$$
$$(f_1) = P_1 + 2P_3 + P_4 + 2P_5 - 2Q,$$
$$(f_2) = 2P_1 + P_2 + P_4 + 2P_6 - 2Q,$$
$$(f_3) = P_1 + 2P_2 + P_3 + 2P_7 - 2Q.$$

Hence $1, f_1, f_2, f_3$ are in $L(2Q)$. It is easily verified that they are linearly independent. This basis of $L(2Q)$ gives the generator matrix

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

of $C_L(\mathcal{X}_1, D_1, 2Q)$. This should be a generator matrix of a $[7, 4, 3]$ code, and indeed it is.

Remark 29 In Proposition 16 we gave a SAG representation of an $H(3, 2)$: $C_L(\mathcal{X}_1, D_1, 2Q)$ is an $H(3, 2)$. As pointed out in Remark 1, we can also give this code as a $C_\Omega(\mathcal{X}_1, D_1, G)$

code, equivalently. Following (an adjusted version of) the proof of [4, Ch.8,Prop.8,p.207], we find that the differential

$$\omega_1 := \frac{z^3}{y^2z + x^3 + x^2z} d\left(\frac{x}{z}\right)$$

has divisor

$$(\omega_1) = L_2 \cdot \mathcal{X}_1 = 2P_2 + P_4 + P_6.$$

Note that $y^2z + x^3 + x^2z$ is the partial derivative to y of the left-hand side of (3). Define the forms

$$H_6 := y^3 + yz^2 + y^2z + x^2z + xyz,$$
$$H_7 := y^3 + z^3 + x^2z + y^2z + xyz.$$

Then

$$H_6 \cdot \mathcal{X}_1 = P_1 + P_4 + Q + U,$$
$$H_7 \cdot \mathcal{X}_1 = P_4 + P_5 + V,$$

where U is the place of degree 7 on $\mathcal{X}_1$ corresponding to the orbit of the $\mathbf{F}_{128}$-rational point $(\gamma^{90} : \gamma^{23} : 1)$, with $Gal(\mathbf{F}_{128}/\mathbf{F}_2)$ acting, and where V is the place of degree 10 on $\mathcal{X}_1$ corresponding to the orbit of the $\mathbf{F}_{1024}$-rational point $(\delta^{1017} : \delta^{159} : 1)$, with $Gal(\mathbf{F}_{1024}/\mathbf{F}_2)$ acting. Here $\mathbf{F}_{128} = \mathbf{F}_2(\gamma)$ with $\gamma^7 + \gamma^3 + 1 = 0$, and $\mathbf{F}_{1024} = \mathbf{F}_2(\delta)$ with $\delta^{10} + \delta^3 + 1 = 0$. Put

$$\omega := \frac{H_6H_7}{H_1L_2L_4}\omega_1.$$

Then $(\omega) = U + V - 2Q - D_1$. Hence ω has a simple pole at P_i and $res_{P_i}(\omega) = 1$ for $i = 1, \ldots, 7$. Define G_1' by $2Q = (\omega) - G_1' + D_1$. Then

$$G_1' = U + V - 4Q.$$

By Remark 1, $C_\Omega(\mathcal{X}_1, D_1, G_1') = C_L(\mathcal{X}_1, D_1, 2Q)$.

Remark 29 In the above we have proved that $H(3, 2)$ has exactly two (WAG) representation classes with $g = 3$. These are $[(\mathcal{X}_1, D_1, G_1)]$ and $[(\mathcal{X}_1, D_1, 2Q)]$, the latter of which is SAG, moreover. This shows that $H(3, 2)$ has more than one WAG representation class.

Lemma 14 *The (SAG) representation $(\mathcal{X}_1, D_1, 2Q)$ is minimal.*

Proof: As noted already at the beginning, after Remark 24, the genus $g(\mathcal{X}_1) = 3$ is minimal. The divisor $2Q$ is base point free, since its degree is $6 \geq 2g$, see [11, p.308,Cor.3.2]. The result follows by Corollary 2.

If $[(\mathcal{X}, D, G)]$ is a *minimal* AG representation class of $H(3, 2)$, then $(g, m) = (3, 6)$ or $(4, 6)$, by Proposition 12 and Table II. By Lemma 8, Lemma 10 and Proposition 16, there is exactly one AG representation class of $H(3, 2)$ with $(g, m) = (3, 6)$, $[(\mathcal{X}_1, D_1, 2Q)]$ namely, and this representation class is *minimal* by Lemma 14. From the next proposition it follows that there exists no AG representation class of $H(3, 2)$ with $(g, m) = (4, 6)$ (minimal or not). To avoid any misunderstandings: the definitions of P_i, Q, etc... that we used until now do not apply to Proposition 17 and Lemma 15 and their proofs.

Proposition 17 *If $(\mathcal{X}, D, G)$ is an AG representation of an $H(3,2)$, then $g(\mathcal{X}) \neq 4$.*

Proof: Suppose that $(\mathcal{X}, D, G)$ is an AG representation of a binary $[7,4,3]$ code, $D = P_1 + \cdots + P_7$ and $g = 4$. The curve $\mathcal{X}$ is not hyperelliptic, since it has more than $2q+2 = 6$ $\mathbf{F}_2$-rational points. If $m = \deg(G) < 6$, then $4 = l(G) = m+1-4+i(G)$, hence $i(G) > 0$, by the Riemann-Roch theorem. But then $l(G) \leq 1 + m/2 < 4$, by Clifford's theorem. Hence $m \geq 6$, and because $m < n = 7$, $m = 6$. So G is a divisor of degree $2g-2$ with $i(G) = 1$. In other words, G is a canonical divisor, that is to say, $G = (\omega_0)$ for a differential ω_0. Because $C_L(\mathcal{X}, D, G)$ is an $H(3,2)$, $C_\Omega(\mathcal{X}, D, G)$ is an $S(3,2)$, see Proposition 1 and Definition 5. By Remark 1, there is a divisor G' on $\mathcal{X}$ such that $G' \sim D$ and $C_L(\mathcal{X}, D, G') = C_\Omega(\mathcal{X}, D, G)$. So $C_L(\mathcal{X}, D, G')$ is a $[7,3,4]$ code.
We claim that

$$l(P_a + P_b + P_c) = 1 \text{ for all } a, b, c \in \{1, \ldots, 7\} \text{ with } a \neq b, a \neq c, b \neq c.$$

The proof of this claim is actually more or less the reverse of the proof of Proposition 15. Namely, write $G' = D + (f_0)$. Suppose that $l(P_a + P_b + P_c) > 1$ for some distinct a, b, c. Let $f_1 \in L(P_a + P_b + P_c)$ with $f_1 \neq 0, 1$. Put $f := f_1/f_0$. Then $f \notin L(G' - D) = L((f_0))$, since otherwise $(f) = -(f_0)$, and consequently $f_1 = f f_0 = 1$, which gives a contradiction by the choice of f_1. On the other hand, $f f_0 = f_1 \in L(P_a + P_b + P_c)$ implies that $(f) \geq -(f_0) - P_a - P_b - P_c = -G' + P_r + P_s + P_t + P_u$, where $P_r + P_s + P_t + P_u = D - P_a - P_b - P_c$. From the above it follows that $f \in L(G') \setminus L(G' - D)$, and that $\alpha_L(f)$ is a nonzero codeword in $C_L(\mathcal{X}, D, G')$ of weight at most three, see Definition 1. This contradicts the fact that $C_L(\mathcal{X}, D, G')$ is a $[7,3,4]$ code.
We proceed with the proof of the proposition. Suppose that there exists an effective divisor E of degree three on $\mathcal{X}$ with $l(E) > 1$. Then E is obviously base point free, see Lemma 11. The morphism

$$\varphi_E : \mathcal{X} \to \mathbf{P}^1$$

has degree three, see Remark 6, and we have $\varphi_E(P_i) \in \mathbf{P}^1(\mathbf{F}_2)$ for $i = 1, \ldots, 7$. Since $\#\mathbf{P}^1(\mathbf{F}_2) = 3$, there exists a $Q \in \mathbf{P}^1(\mathbf{F}_2)$ with at least three points in $\varphi_E^{-1}(Q) \cap \{P_1, \ldots, P_7\}$, P_a, P_b, P_c say. Since $\deg(\varphi_E) = 3$, the pull back $\varphi_E^*(Q)$ of Q under φ_E is equal to $P_a + P_b + P_c$, see [11, p.138,Prop.6.9]. This implies that $E \sim P_a + P_b + P_c$, and hence that $l(P_a + P_b + P_c) = l(E) > 1$. But this contradicts the previous claim. We conclude that $l(E) = 1$ for all $E \geq 0$ with $\deg(E) = 3$. By the following lemma, however, this is not true, and hence the assumption that $(\mathcal{X}, D, G)$ is an AG representation of an $H(3,2)$ is wrong. This proves the proposition.

Lemma 15 *If $\mathcal{X}$ is a nonsingular, absolutely irreducible curve over $\mathbf{F}_2$ of genus 4 with at least seven $\mathbf{F}_2$-rational points, then there exists an effective divisor E on $\mathcal{X}$ with $\deg(E) = 3$ and $l(E) = 2$.*

Proof: Let K be a canonical divisor and let P_0 be a rational point on $\mathcal{X}$. We have $l(K) = 6 + 1 - 4 + 1 = 4$, by Riemann-Roch. Put $G := K - P_0$. Then $\deg(G) = 5$. Since $\mathcal{X}$

is not hyperelliptic, K is very ample, see [11, p.341,Prop.5.2]. Hence $l(G) = l(K) - 1 = 3$ and G is base point free. Let $\mathcal{X}_0$ be the reduced image of $\mathcal{X}$ under the morphism

$$\varphi_G : \mathcal{X} \to \mathbf{P}^2,$$

see Remark 6. We have

$$5 = \deg(\varphi_G) \cdot \deg(\mathcal{X}_0).$$

As pointed out in Remark 6, $\mathcal{X}_0$ is not a line, hence $\deg(\mathcal{X}_0) \neq 1$. It follows that $\deg(\mathcal{X}_0) = 5$, and that $\deg(\varphi_G) = 1$, i.e. φ_G is a birational morphism. We have

$$4 = g(\mathcal{X}) = g(\mathcal{X}_0) = \frac{1}{2}(5-1)(5-2) - \sum_{P \in \mathcal{X}_0} \delta_P \deg(P), \tag{5}$$

where δ_P is the delta invariant at P, see [18]. We have $\delta_P \geq m_P(m_P - 1)/2$, where m_P is the multiplicity of $\mathcal{X}_0$ at P. From (5) it follows that

$$\sum_{P \in \mathcal{X}_0} \delta_P \deg(P) = 2. \tag{6}$$

Hence $\mathcal{X}_0$ has two rational singular points, each with delta invariant 1, or one rational point with delta invariant 2, or one singular point of degree two with delta invariant 1. In every case, the singular point(s) have multiplicity 2 (since if $m_P \geq 3$, then $\delta_P \geq 3(3-1)/2 = 3$, contradicting (6)).

We claim that $\mathcal{X}_0$ has a rational singular point. To prove this, suppose $\mathcal{X}_0$ has no such point. Then $\mathcal{X}_0$ has a singular point Q of degree 2. There is exactly one line through Q in $\mathbf{P}^2$, defined over $\mathbf{F}_2$. We call this line L_1. By Bézout's theorem, L_1 intersects $\mathcal{X}_0$ at 5 points, counted with multiplicities. The intersection multiplicity at Q is even and at least 4, hence equal to 4, and there is exactly one rational point P_1 in $L_1 \cap \mathcal{X}_0$. Let L_2 and L_3 be the other two lines through P_1 in $\mathbf{P}^2$, defined over $\mathbf{F}_2$. Then φ_G maps every rational point of $\mathcal{X}$ to a rational point in $(L_1 \cap \mathcal{X}_0) \cup (L_2 \cap \mathcal{X}_0) \cup (L_3 \cap \mathcal{X}_0)$. But $L_1 \cap \mathcal{X}_0$ contains exactly one rational point, P_1 namely, and $L_2 \cap \mathcal{X}_0$ and $L_3 \cap \mathcal{X}_0$ each contain at most two rational points not equal to P_1. Hence φ_G maps (at least) 7 rational points of $\mathcal{X}$ to at most 5 rational points of $\mathcal{X}_0$. Thus there are two rational points Q_1, Q_2 on $\mathcal{X}$ such that $\varphi_G(Q_1) = \varphi_G(Q_2)$, and $\varphi_G(Q_1)$ is a rational singular point of $\mathcal{X}_0$, a contradiction. This proves the claim.

Thus $\mathcal{X}_0$ is a plane model of degree 5 of $\mathcal{X}$, with at least one rational singular point, which we call Q_0. As noted earlier in the proof, the multiplicity of $\mathcal{X}_0$ at Q_0 is 2. Hence there is an effective divisor B of degree 2 such that

$$\mathcal{X}_0 \cdot M \geq B$$

for every line M through Q_0, defined over $\mathbf{F}_2$. Besides Q_0, there is at least one other rational point on $\mathcal{X}_0$, since otherwise φ_G would map (at least) 7 rational points of $\mathcal{X}$ to Q_0, and $m_{Q_0} \geq 7 > 2$, a contradiction. Let Q_0' be such another rational point on $\mathcal{X}_0$. Let

M_1 be the line through Q_0 and Q_0', and let M_2 be one of the other two lines through Q_0 defined over $\mathbf{F}_2$. Then $Q_0' \notin M_2$. Put

$$R_i := \mathcal{X}_0 \cdot M_i - B$$

for $i = 1, 2$. Then $R_i \geq 0$ and $\deg(R_i) = 3$ for both i. Put $f := M_2/M_1$. Then $f \in L(R_1)$, $(f) = R_2 - R_1$, and f is not a constant, since it has a pole at Q_0'. Hence $l(R_1) \geq 2$. In fact, we have equality, by Riemann-Roch and Clifford's theorem. To prove the proposition, choose $E := \varphi_G^*(R_1)$, the pull back of R_1 under φ_G.

We summarize our main results concerning the Hamming codes in the following theorem.

Theorem 6 *a) $H(1, q)$ and $H(2, q)$ are SAG, for every q.*
b) $H(3, 2)$ is SAG.
c) $H(r, q)$ is not AG if $r \geq 3$ and $(r, q) \neq (3, 2)$.
d) $[(\mathcal{X}_1, D_1, 2Q)]$ is a minimal SAG representation class of $H(3, 2)$.
e) $[(\mathcal{X}_1, D_1, 2Q)]$ is the only minimal AG representation class of $H(3, 2)$.
Here $\mathcal{X}_1$ is defined by (3), D_1 is defined after Lemma 8, and Q is defined in Remark 26.

B. Another example

Let C be the binary [6,4,2]-code with generator matrix

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

This code was mentioned by Katsman and Tsfasman in [13], where they more or less raised the question whether this code is algebraic-geometric. We shall give the answer to this question here.

Proposition 18 *The code C is SAG.*

Proof: Let $\mathcal{X}_2$ be the plane projective curve of degree four defined over $\mathbf{F}_2$ by the equation

$$xyz^2 + (x^3 + x^2y + y^3)z + x^3y + xy^3 = 0.$$

As is easily verified, this curve has exactly one singularity: the point $P := (0 : 0 : 1)$ is an ordinary double point. The tangents to $\mathcal{X}_2$ at P are $x = 0$ and $y = 0$. It follows, by Bézout's theorem, that $\mathcal{X}_2$ is absolutely irreducible. The curve is a hyperelliptic curve, of genus 2. Besides the singular point P, there are four other rational points on $\mathcal{X}_2$: $P_1 := (1 : 0 : 0)$,

$P_2 := (1:1:0)$, $P_3 := (0:1:0)$, and $P_4 := (1:1:1)$. The singular point P gives two rational points on the nonsingular model of $\mathcal{X}_2$. Or, to put it differently, it corresponds to two places (=discrete valuation rings) of degree one in the function field of $\mathcal{X}_2$ over $\mathbf{F}_2$. We call these places P_5 and P_6. Let L and M be the lines $z = 0$ and $x+y+z = 0$, respectively. The line L is the tangent to $\mathcal{X}_2$ at P_2. We have

$$L \cdot \mathcal{X}_2 = P_1 + 2P_2 + P_3.$$

The only rational point in $M \cap \mathcal{X}_2$ is P_2, and the intersection at this point is transversal. Define the divisor G_2 by

$$M \cdot \mathcal{X}_2 = P_2 + G_2.$$

Then $G_2 \geq 0$, $\deg(G_2) = 3$ and $\mathrm{supp}(G_2) \cap \mathrm{supp}(D_2) = \emptyset$. Here we have put $D_2 := P_1 + P_2 + \cdots + P_6$. (Although we do not need this, it follows that G_2 is a place of degree three. This place turns out to be $\{(1:\alpha:1+\alpha), (1:\alpha^2:1+\alpha^2), (1:\alpha^4:1+\alpha^4)\}$, where $\mathbf{F}_8 = \mathbf{F}_2(\alpha)$ with $\alpha^3 + \alpha + 1 = 0$).

By the Riemann-Roch theorem, $l(G_2) = 3 + 1 - 2 = 2$. The rational functions 1 and L/M $(= z/(x+y+z))$ are in $L(G_2)$, and they (obviously) form a basis. This basis of $L(G_2)$ gives

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

as a generator matrix of the binary [6,2,3] code $C_L(\mathcal{X}_2, D_2, G_2)$. Since $2 = 2g - 2 < 3 = \deg(G_2) < 6 = n$, $C_L(\mathcal{X}_2, D_2, G_2)$ is SAG. Since $C_L(\mathcal{X}_2, D_2, G_2)^\perp = C$, C is SAG too, by Corollary 1. This completes the proof of the proposition.

Acknowledgment

We would like to thank A.B. Sørensen, for the use of his zeta function computer program, and C. Faber for an indication of the result of Lemma 7.

References

[1] E. Arbarello, M. Cornalba, P.H. Griffiths, J. Harris, Geometry of algebraic curves, volume I. Grundlehren der mathematischen Wissenschaften **267**. Springer-Verlag, 1985.

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

[3] P. Delsarte, J.M. Goethals and F.J. MacWilliams, "On generalized Reed-Muller codes and their relatives", Information and Control **16** (1970), pp. 403-442.

[4] W. Fulton, Algebraic curves. Benjamin, Reading, Massachusetts, 1969.

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

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

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

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

[9] V.D. Goppa, Geometry and codes. Mathematics and its applications, Soviet series **24**. Kluwer Ac. Publ., Dordrecht, The Netherlands, 1988.

[10] J.P. Hansen and H. Stichtenoth, "Group codes on certain algebraic curves with many rational points", AAECC **1** (1990), pp. 67-77.

[11] R. Hartshorne, Algebraic geometry. Graduate Texts in Math. **52**. Springer-Verlag, Berlin Heidelberg New York, 1972.

[12] S. Iitaka, Algebraic geometry, an introduction to birational geometry of algebraic varieties. Graduate Texts in Math. **76**, Springer-Verlag, New York Heidelberg Berlin, 1982.

[13] G.L. Katsman and M.A. Tsfasman, "Spectra of algebraic-geometric codes", Probl. Peredachi Inform. **23** (4) (1987), pp. 19-34. Translation: Probl. Inform. Transmission **23** (4), (1987), pp. 262-275.

[14] G. Lachaud, "Les codes géométriques de Goppa", Sem. Bourbaki 1984-1986, no. 641, in Astérisque **133-134** (1986), pp. 189-207.

[15] J.H. van Lint, Introduction to coding theory. Graduate Texts in Math. **86**. Springer-Verlag, Berlin Heidelberg New York, 1982.

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

[17] F.J. McWilliams and N.J.A. Sloane, The theory of error-correcting codes. North-Holland Math. Library **16**. North-Holland, Amsterdam, 1977.

[18] J.-P. Serre, Algebraic groups and class fields. Graduate Texts in Math. **117**. Springer-Verlag, Berlin Heidelberg New York, 1988; = Translation of: Groupes algébriques et corps de classes. Hermann, Paris, 1959.

[19] J.-P. Serre, "Nombre de points d'une courbe algébriques sur $\mathbf{F}_q$", Séminaire Th. Nombres, Bordeaux, 1982-1983, exp. no. 22; =Oeuvres, III, no. 129, p. 664-668.

[20] J.-P. Serre, "Sur le nombre des points rationels d'une courbe algébrique sur un corps fini", C.R. Acad. Sci. Paris **296** (1983), 397-402; =Oeuvres, III, no. 128, pp. 658-663.

[21] H. Stichtenoth, "Self-dual Goppa codes", J. Pure Applied Alg. **55** (1988), pp. 199-211.

[22] M.A. Tsfasman and S.G Vlăduţ, Algebraic-geometric codes. Kluwer Ac. Publ., Dordrecht, The Netherlands, to appear.

LIST OF TABLE CAPTIONS

Table I. Some known values of $N_q(g)$.

Table II. Restrictions on binary AG $[n, k]$ codes, see Proposition 12.

Table III. The $\mathbf{F}_2$-rational points P_i on the curve $\mathcal{X}_1$, the tangents L_i to $\mathcal{X}_1$ at these points, and the intersection divisors $L_i \cdot \mathcal{X}_1$.

Table IV. This table is used in the proof of Proposition 16. All $E \in \Lambda_1$ with $\#\overline{E} > 1$ are listed.