NOTES ON ALGEBRAIC-GEOMETRIC CODES

MASSIMO GIULIETTI

Introduction

Ideas from algebraic geometry became useful in coding theory after Goppa's construction [8]. He had the beautiful idea of associating to a curve $\mathcal{X}$ defined over $\mathbf{F}_q$, the finite field with q elements, a code C. This code, called *Algebraic-Geometric (AG) code*, is constructed from two divisors D and G on $\mathcal{X}$, where one of them, say D, is the sum of n distinct $\mathbf{F}_q$-rational points of $\mathcal{X}$. It turns out that the minimum distance d of C satisfies

$$d \geq n - deg(G)\,.$$

This is one of the main features of Goppa's construction. In general there is no lower bound available on the minimum distance of a code. This bound is meaningful only if n is large enough, then it is of considerable interest to do research on curves with "many rational points"; see e.g. [6].

The purpose of these notes is not to survey the vast body of literature on AG codes but just to provide a short and possibly plain introduction to this subject. Hence, we will bypass most of all the underlying Algebraic Geometry. This has two major drawbacks: firstly we can deal only with a limited class of AG codes, secondly the deep theorems on which AG codes rely are presented without proof. Nonetheless, we believe that such presentation is somehow more useful to the beginning student, and we hope that it may give some motivation to learn the subject in all its depth and beauty.

These notes are based on a series of lectures given in May 2003 at the Mathematical Department of KTH in Stockholm.

Contents.

(1) Linear codes
(2) Reed-Solomon codes
(3) Algebraic curves
(4) Algebraic-Geometric codes
(5) Bounds on linear codes
(6) One-point AG codes
(7) MDS codes and Almost MDS codes

1. Linear codes

In this section we briefly summarize some basic material regarding linear codes on the alphabet $\mathbf{F}_q$, the finite field of order q; for comprehensive treatises see [17], [15], [16], [18], [25], [27].

Let n be a positive integer.

Definition 1.1. A *code* is any non-empty subset of $\mathbf{F}_q^n$. The code is called *linear* if it is an $\mathbf{F}_q$-linear subspace of $\mathbf{F}_q^n$. The number n is the *length* of the code.

Definition 1.2. The *Hamming distance* d on $\mathbf{F}_q^n \times \mathbf{F}_q^n$ is given by

$$d(\vec{x}, \vec{y}) = \#\{i : x_i \neq y_i\},$$

where $\vec{x} = (x_1, \ldots, x_n)$ and $\vec{y} = (y_1, \ldots, y_n)$. The *weight* of $\vec{x}$ is defined by

$$w(\vec{x}) := d(\vec{x}, \vec{o}),$$

where $\vec{o} := (0, \ldots, 0)$.

Remark 1.3. The function d is a metric on $\mathbf{F}_q^n \times \mathbf{F}_q^n$.

Definition 1.4. The *minimum distance* of a code $C \subseteq \mathbf{F}_q^n$ is given by

$$d(C) := \min\{d(\vec{x}, \vec{y}) : \vec{x}, \vec{y} \in C, \vec{x} \neq \vec{y}\}.$$

Remark 1.5. For $C \subseteq \mathbf{F}_q^n$ a linear code we have that

$$d(C) = \min\{w(\vec{x}) : \vec{x} \in C \setminus \{\vec{o}\}\}.$$

Definition 1.6. Let $C \subseteq \mathbf{F}_q^n$ be a linear code of dimension k. A *generator matrix* of C is a $k \times n$ matrix whose rows form an $\mathbf{F}_q$-base of C.

Definition 1.7. Let $C \subseteq \mathbf{F}_q^n$ be a code. The *dual code* of C is the code $C^\perp$ defined by

$$C^\perp := \{\vec{x} \in \mathbf{F}_q^n : \langle \vec{x}, \vec{y} \rangle = 0, \forall\, \vec{y} \in C\},$$

where for $\vec{x} = (x_1, \ldots, x_n), \vec{y} = (y_1, \ldots, y_n)$, $\langle \vec{x}, \vec{y} \rangle := \sum_{i=1}^n x_i y_i$ is the usual bilinear form on $\mathbf{F}_q^n \times \mathbf{F}_q^n$.

Note that $C^\perp$ is indeed a linear code. For $\vec{x} \in \mathbf{F}_q^n$, let $\vec{x}^t$ denote its transpose.

Lemma 1.8. *Let $C \subseteq \mathbf{F}_q^n$ a linear code of dimension k and M a generator matrix of C. Then*

(1) $C^\perp = \{\vec{x} \in \mathbf{F}_q^n : M\vec{x}^t = \vec{o}\}$;
(2) $C^\perp$ *has dimension* $n - k$.

Proof. (1) Let $\vec{v}_1, \ldots, \vec{v}_k$ be the rows of M. Then (1) is an easy consequence of the following facts:

- for $\vec{x} \in \mathbf{F}_q^n$, $M\vec{x}^t = (\langle \vec{v}_1, \vec{x} \rangle, \ldots, \langle \vec{v}_k, \vec{x} \rangle)$;

- for $\vec{x} \in C$, there exist $a_1, \ldots, a_k \in \mathbf{F}_q$ such that $\vec{x} = \sum_{i=1}^{k} a_i \vec{v}_i$.

(2) By (1), $C^\perp$ is the kernel of the linear map $\vec{x} \mapsto M\vec{x}^t$ whose rank is k. So (2) follows from basic linear algebra. □

Corollary 1.9. *Let C be a linear code and H a generator matrix of $C^\perp$. Then:*

(1) $C = (C^\perp)^\perp$;
(2) $C = \{\vec{x} \in \mathbf{F}_q^n : H\vec{x}^t = \vec{o}\}$.

Proof. (1) Clearly $C \subseteq (C^\perp)^\perp$ and by Lemma 1.8(2), both codes $(C^\perp)^\perp$ and C have the same dimension. This implies (1).

(2) The assertion follows from (1) and Lemma 1.8(1). □

Definition 1.10. The *redundancy* of a k-dimensional linear code in $\mathbf{F}_q^n$ is $n - k$.

Definition 1.11. A *parity check* matrix of a linear code is any generator matrix of its dual.

Lemma 1.12. *Let C be a linear code and H a parity check matrix of C.*

(1) *There exists $\vec{x} \in C$ of weight w if and only if there exist w columns of H which are $\mathbf{F}_q$-linearly dependent.*
(2) *We have*

$$d(C) = \min\{w \in \mathbf{Z}^+ : \exists\, w \text{ columns } \mathbf{F}_q\text{-linearly dependent in } H\}\,.$$

Proof. (1) It follows from Corollary 1.9(2) together with the fact that $H\vec{x}^t = \sum_{i=1}^{n} x_i \vec{H}_i$, where $\vec{x} = (x_1, \ldots, x_n)$ and $\vec{H}_1, \ldots, \vec{H}_n$ are the columns of H.

(2) The assertion follows from (1) and the definition of $d(C)$. □

Corollary 1.13. (Singleton Bound) *For an $\mathbf{F}_q$-linear code of length n, dimension k and minimum distance d,*

$$d - 1 \leq n - k\,.$$

Proof. By Lemma 1.12(2) any $d - 1$ columns of H, H being a parity check matrix of C, are $\mathbf{F}_q$-linearly independent. Since H has rank $n - k$, the assertion follows. □

Definition 1.14. An $\mathbf{F}_q$-linear code of length n, dimension k and minimum distance d is called *maximum distance separable* (MDS) if $d - 1 = n - k$.

Proposition 1.15. *The dual code of an MDS code is MDS.*

Proof. Let H be a parity check matrix of an MDS code C of length n and dimension k. The generic element of $C^\perp$ then can be written as

$$\vec{y}H = (\langle \vec{H}_1, \vec{y} \rangle, \ldots, \langle \vec{H}_n, \vec{y} \rangle)$$

where $\vec{y}$ ranges over $\mathbf{F}_q^{n-k}$ and $\vec{H}_i$ is the i^{th} column of H. As C is MDS, any $n-k$ columns of H are linearly independent. Hence, the maximum number of columns of H which are solutions of the linear equation $\langle \vec{x}, \vec{y} \rangle = 0$ is $n-k-1$. This means that the minimum distance of $C^\perp$ is at least $n-(n-k-1) = n-(n-k)+1$, and hence $C^\perp$ is MDS. $\square$

Remark 1.16. For a linear code C, the Singleton bound is independent of q. A restriction on the parameters n, k and d of C which involves q as well can be obtain as follows.

Let t be the largest integer not exceeding $(d-1)/2$. For $\vec{x} \in \mathbf{F}_q^n$, let

$$B(\vec{x}, t) := \{\vec{y} \in \mathbf{F}_q^n : d(\vec{y}, \vec{x}) \leq t\}\,.$$

Then it is easy to see that $V_q(n,t) := \#B(\vec{x}, t) = \sum_{i=1}^{t} \binom{n}{i}(q-1)^i$, and that $B(\vec{x}_1, t) \cap B(\vec{x}_2, t) = \emptyset$ provided that $\vec{x}_1, \vec{x}_2$ are two different elements of C. Then

$$\cup_{\vec{x} \in C} B(\vec{x}, t) \subseteq \mathbf{F}_q^n\,,$$

and we obtain the so-called "Hamming bound"

$$V_q(n,t)\#C \leq q^n\,.$$

Notice that this bound is valid for any code C and if C is linear of dimension k, then $\#C = q^k$.

2. Reed-Solomon codes

As a motivation for the construction of AG codes, in the following examples we consider Reed-Solomon codes over $\mathbf{F}_q$. This important class of codes has been well-known in coding theory for a long time. AG codes are a very natural generalization of Reed-Solomon codes.

Let q be a prime power, n and k be integers such that $1 \leq k \leq n \leq q$. Let $\mathbf{F}_q[X]$ be the ring of polynomials in one variable with coefficients in $\mathbf{F}_q$. Now set

$$L_k := \{f \in \mathbf{F}_q[X] : deg(f) \leq k-1\} \cup \{0\}\,,$$

and for n distinct elements $P_1, \ldots, P_n$ of $\mathbf{F}_q$, consider the following $\mathbf{F}_q$-linear map:

$$\begin{aligned} e = e_{P_1,\ldots,P_n} : L_k &\to \mathbf{F}_q^n \\ f &\mapsto (f(P_1), \ldots, f(P_n))\,. \end{aligned}$$

We have that e is injective since a non-zero polynomial in L_k can have at most $k-1$ zeros. Then the code $C := e(L_k)$ has dimension k. The code C is called a *Reed-Solomon code* (RS code for short). Let $\vec{x} = (f(P_1), \ldots, f_n(P)) \in C$ and assume that $w(\vec{x}) = w$. Then f has $n-w$ zeros and so $n-w \leq k-1$. In particular, $n-d \leq k-1$, where d is the minimum distance of C. Therefore $n-k \leq d-1$ and so, by Corollary 1.13, we must

have $n-k=d-1$, i.e., C is an MDS code. Note that as $1, X, \ldots, X^{k-1}$ is a basis of L_k, a generator matrix of C is the following:

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ P_1 & P_2 & \ldots & P_n \\ P_1^2 & P_2^2 & \ldots & P_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ P_1^{k-1} & P_2^{k-1} & \ldots & P_n^{k-1} \end{pmatrix}$$

Let q be a prime power, n and k be integers such that $1 \leq k \leq n \leq q$. Also, let $P_1, \ldots, P_n$ be distinct elements of $\mathbf{F}_q$, and let $\vec{v} = (v_1, \ldots, v_n)$ where the v_i's are non-zero (not necessarily distinct) elements of $\mathbf{F}_q$. Then the code consisting of all vetcors

$$(v_1 f(P_1), \ldots, v_n f(P_n))$$

with $f \in \mathbf{F}_q[X]$ and $deg(f) \leq k-1$, is called a *Generalized Reed Solomon code* (GRS code for short). Note that in the case where $\vec{v} = (1, 1, \ldots, 1)$ such a code is a Reed Solomon code.

3. Algebraic curves

For comprehensive treatises on algebraic curves we refer to [10], [25], [16], [8], and [23]. According to the purpose of these notes, we will limit ourselves to deal with the simplest type of algebraic curve, that is with plane smooth curves.

Let K be a field and let $F(X,Y)$ be a polynomial of two variables over K. A point (a,b) lying in the plane over K is called root of the polynomial if $F(a,b)=0$. All these roots define an *affine curve* over K. Actually, one considers all points with coordinates in the algebraic closure of K. In the case $K=\mathbf{F}_q$, this means that a point of the affine curve is (a,b) such that $a,b \in \mathbf{F}_{q^m}$ for some positive integer m, and $F(a,b)=0$. Points of the curve with $(a,b) \in K$ are said to be rational over K (or K-rational).

Given a homogenous polynomial $F(X,Y,Z)$ over K, the *projective curve* defined by F is the of points $P(a:b:c)$ lying in the projective plane over the algebraic closure of K such that $F(X,Y,Z)=0$. Every such a curve corresponds to three affine curves resulting from dehomogenization:

$$F(1,Y,Z)=0, \qquad F(X,1,Y)=0, \qquad F(X,Y,1)=0.$$

Conversely, an affine curve converts to a projective one under homogenization: $Z^d F(X/Z, Y/Z)$, where d is the degree of F.

Example 3.1. The affine curve defined by $Y^2 - X^2(X+1)$ is associated to the projective curve of equation $Y^2Z - X^3 - X^2Z = 0$. The projective curve defined by $X^5 + Y^5 - Z^5$ is associated with the affine curve of equation $X^5 + Y^5 = 1$.

An affine (resp. projective) curve is called irreducible if $F(X,Y)$ (resp. $F(X,Y,Z)$) cannot be written as a product of two polynomial of degree bigger than zero. Associating $F(X,Y,Z)$ to $F(X,Y,1)$ gives a one-to-one correspondence between the set of all irreducible projective curves and that of irreducible affine curves.

A point $P=(a:b:c)$ of an irreducible projective curve $\mathcal{X}$ defined by $F(X,Y,Z)$ is said to be singular if all the derivatives F_X, F_Y, F_Z are zero at P. Otherwise P is called simple. If all points are simple, then $\mathcal{X}$ is said to be non-singular (or smooth). Calculations involving singularity depend strongly on the characteristic of the ground field K.

Example 3.2. Let K be any field of characteristic two and let $\mathcal{X}$ be the curve defined over K by $F=Y^2Z-X^3+X^2Z$. Then $F_X=X^2$, $F_Y=0$, $F_Z=Y^2-Z^2=(Y-X)^2$. Hence $P=(a:b:c)$ is singular if and only if $a=0, b=a$, that is $P=(0:0:1)$ is the only singular point of $\mathcal{X}$.

Example 3.3. Let K be any field, and let $\mathcal{X}$ be the curve defined over K by $F=X^5+Y^5+Z^5$. Then $F_X=5X^4$, $F_Y=5Y^4$, $F_Z=5Z^4$. If the characteristic p of K is different from 5, then $\mathcal{X}$ is smooth. Otherwise, every point of $\mathcal{X}$ is singular. Actually, for $p=5$, $\mathcal{X}$ is reducible as $F=(X+Y+Z)^5$.

Example 3.4 (Klein quartic)**.** Let K be any field of characteristic two, and let $\mathcal{X}$ be the curve defined over K by $F=X^3Y+Y^3Z+Z^3X$. Then $F_X=X^2Y+Z^3$, $F_Y=Y^2Z+X^3$, $F_Z=Z^2X+Y^3$. Assume that $P=(a:b:c)$ is a singular point of $\mathcal{X}$. Then (i) $a^2b=c^3$ together with (ii) $a^3b+b^3c+c^3a=0$ yield $b^3c=0$. If $b=0$, then (i) gives $c=0$ and hence (iii) $F_Y(P)=0$ yields $a=0$. If $c=0$, then $b=0$ by (i), and again $a=0$ by (iii). This means that $\mathcal{X}$ is smooth.

Example 3.5 (Hermitian curve)**.** Let K be a finite field with q^2 elements, with q a prime power. Let $\mathcal{X}$ be the curve defined over K by $F=Y^qZ+YZ^q-X^{q+1}$. As $F_X=-X^q$, $F_Y=Z^q$ and $F_Z=Y^q$ the curve $\mathcal{X}$ is smooth.

Given a polynomial F, establishing whether the associated curve is irreducible is not easy in general. There exist several irreducibility criterions, which we will not deal with here. We only remind the fact that smooth curves are irreducible.

From now on, by the word curve we will mean a *projective smooth curve defined over* K.

3.1. **Rational functions.** Let $\mathcal{X}$ be the curve defined by $F(X,Y,Z)$. On the points of $\mathcal{X}$, any two polynomials that differ by multiples of F have the same value. So, as far as $\mathcal{X}$ is concerned, they are the same. We shall give a definition of function that reflects this idea. Roughly speaking, a *rational function* of $\mathcal{X}$ is the ratio $f=A(X,Y,Z)/B(X,Y,Z)$ of two homogenous polynomials of the same degree up to factorization modulo $F(X,Y,Z)$. A precise definition is the following. Let I be the ideal of $K[X,Y,Z]$ generated by F. As $\mathcal{X}$ is irreducible, I is a prime ideal and then the quotient ring $K[X,Y,Z]/I$ is an integral

domain. An element g in $K[X,Y,Z]/I$ is said to be a form of degree d if $g = G + I$, for some homogenous polynomial $G \in K[X,Y,Z]$ with $deg(G) = d$. The set of rational functions of $\mathcal{X}$ is

$$K(\mathcal{X}) = \{f = g/h \mid f, g \in K[X,Y,Z]/I \text{ are forms of the same degree and } h \neq 0\},$$

which is a subfield of the field of fractions of $K[X,Y,Z]/I$.

A rational function f is *defined* at a point P, if there exists a representation $f = A/B$ such that $B(P) \neq 0$. In this case one can evaluate the function at P, that is $f(P) = A(P)/B(P)$. Note that this evaluation does not depend on the representation of f.

Example 3.6. Let $\mathcal{X}$ be the curve defined by $F = Y^2Z - YZ^2 + X^3 - X^2Z$ over the field $\mathbf{F}_2$. Consider the rational function f represented by $(Y^2 + YZ)/ZX$. Is f defined at the point $P = (0:0:1) \in \mathcal{X}$? It does not seem so, but actually f is represented by $(X^2 - XZ)/Z^2$ as well. In fact, $Z^2(Y^2 + YZ) - ZX(X^2 - XZ) \in I$ as $Z^2(Y^2 + YZ) - ZX(X^2 - XZ) = ZF$. Therefore f is defined at P and $f(P) = 0$.

Given a point P, let O_P be the ring of all rational functions defined at P. It is easy to see that O_P is an integral domain, and that $K(\mathcal{X})$ is the field of fractions of O_P. Moreover, it can be proved that $M_P := \{f \in O_P \mid f(P) = 0\}$ is a principal ideal. Any generator of M_P is called a *local parameter* at P.

Proposition 3.7. *Let $P = (a:b:c)$ be a point of a curve $\mathcal{X}$ defined by $F(X,Y,Z)$. Assume $c \neq 0$. Let $f = L_1(X,Y,Z)/L_2(X,Y,Z)$ be a rational function in M_P, such that $deg(L_1) = deg(L_2) = 1$, $L_2(P) \neq 0$, and L_1 is not a (constant) multiple of $F_X(P)X + F_Y(P)Y + F_Z(P)Z$. Then f is a local parameter at P.*

Given a point P of $\mathcal{X}$, let t be a local parameter at P. Then for any $f \in K(\mathcal{X})$, $f \neq 0$ there exists a unique integer m such that $f = t^m u$, where $u \in O_P \setminus M_P$. Such an integer m is called the *valuation of f at P* and it is denoted by $v_P(f)$. Note that the elements in O_P are those rational functions f such that $v_P(f) \geq 0$, whereas M_P consists of those with $v_P(f) > 0$.

Valuations have the three following basic properties, whose proofs are left to the reader as an easy exercise:

Proposition 3.8.
(1) *$v_P(fg) = v_P(f) + v_P(g)$ for any $P \in \mathcal{X}$, and for any $f, g \in K(\mathcal{X})$ (and hence $v_P(f^m) = mv_P(f)$ for any integer m);*
(2) *$v_P(f+g) \geq min\{v_P(f), v_P(g)\}$ for any $P \in \mathcal{X}$, and for any $f, g \in K(\mathcal{X})$; if $v_P(f) \neq v_P(g)$ then equality holds;*
(3) *$v_P(a) = 0$ for any $P \in \mathcal{X}$, and for any $a \in K$.*

A point P is said to be a zero of multiplicity m if $v_P(f) = m > 0$, a pole of multiplicity $-m$ if $v_P(f) = m < 0$.

Example 3.9. Let K be any field and let $\mathcal{X}$ be the curve defined by Y (that is, the X-axis). The points of $\mathcal{X}$ are $P_a = (a : 0 : 1)$, with a ranging over the algebraic closure of K, and $P_\infty = (1 : 0 : 0)$. Let $f = X^2/Z^2 \in K(\mathcal{X})$. Clearly f is defined at P_a for any a, and $f(P_a) = a$. Hence, among the P_a's, the only zero of f is P_0. By Proposition 3.7 the function $g = X/Z$ is a local parameter at P_0. As $f = g^2$, we have that $v_{P_0}(f) = v_{P_0}(g^2) = 2v_{P_0}(g) = 2$, that is P_0 is a zero of f of multiplicity two. Now, note that by Proposition 3.7, g^{-1} is a local parameter at P_∞. Hence, $v_{P_0}(f) = v_{P_0}(g^2) = 2v_{P_0}(g) = -2$, meaning that P_∞ is a pole of f of multiplicity two.

Example 3.10. Let $K = \mathbb{R}$ and let $\mathcal{X}$ be the curve defined by $X^2 + Y^2 - Z^2$ (that is the unit circle). Let f be the rational function represented by $X(X - Z)^2/Z(Y - Z)^2$. What are the valuation of f at the points $P_1 = (1 : 0 : 1)$ and $P_2 = (0 : 1 : 1)$? Write $f = u_1 u_2^2$, where $u_1 = X/Z$ and $u_2 = (X - Z)/(Y - Z)$. As u_1 is defined at P_1 and $u_1(P_1) = 1$ we have $v_{P_1}(u_1) = 0$. To compute $v_{P_1}(u_2)$ note that in $K(\mathcal{X})$ the following relation holds: $(X - Z)(X + Z)/(Y - Z)^2 = Y^2/(Y - Z)^2$, that is $u_2 = h_1 h_2$ where $h_1 = Y/(Y - Z), h_2 = Y/(X + Z)$. By Proposition 3.7 both h_1 and h_2 are local parameters at P_1, hence $v_{P_1}(f) = v_{P_1}(u_1) + 2v_{P_1}(h_1 h_2) = 0 + 2 + 2 = 4$, that is P_1 is a zero of f of multiplicity 4. On the other hand, by Proposition 3.7 u_1 is a local parameters at P_2. In $K(\mathcal{X})$, $(Y - Z)(Y + Z)/(X - Z)^2 = -X^2/(X - Z)^2$, that is $u_2^{-1} = g_1 g_2$ where $g_1 = -X/(X - Z)$, $g_2 = X/(Y + Z)$. We can use Proposition 3.7 again to state that both g_1 and g_2 are local parameters at P_2. To sum up, we have that $v_{P_2}(f) = v_{P_2}(u_1) + v_{P_2}(g_1^{-2} g_2^{-2}) = 1 - 2 - 2 = -3$. Hence P_2 is a pole of f of multiplicity 3.

Theorem 3.11. *Any non-zero $f \in K(\mathcal{X})$ has the same (finite) number of zeros and poles, each of them counted with multiplicity.*

3.2. **Divisors.** The free abelian group generated by the points of $\mathcal{X}$ is called the divisor group of $\mathcal{X}$. The elements of this group are called *divisors* of $\mathcal{X}$. In other words, a divisor D is a finite formal sum of points of $\mathcal{X}$, that is $D = \sum_{P \in \mathcal{X}} n_p P$, where n_P is an integer equal to 0 for all but a finite number of points of $\mathcal{X}$.

The *support* of D is defined by $supp(D) := \{P \in \mathcal{X} \mid n_P \neq 0\}$. Two divisors $D = \sum_{P \in \mathcal{X}} n_p P$ and $D' = \sum_{P \in \mathcal{X}} n'_p P$ are added in the natural way

$$D + D' := \sum_{P \in \mathcal{X}} (n_p + n'_P) P \, .$$

The zero element of the group divisor is $\sum_{P \in \mathcal{X}} n_P P$ with $n_P = 0$ for any $P \in \mathcal{X}$. It will be denoted by 0.

A partial ordering on the group divisor is defined by

$$D \leq D' \Leftrightarrow n_P \leq n'_P \text{ for any } P \in \mathcal{X}.$$

If $n_P \geq 0$ for any $P \in \mathcal{X}$ we call D *positive* or *effective*. The *degree* of D is the sum of all integers n_P, that is $deg(D) = \sum_{P \in \mathcal{X}} n_p$.

We will mainly be concerned with a subgroup of the group divisor. A K-*divisor* is a divisor $D = \sum_{P \in \mathcal{X}} n_P P$ such that $n_P = n'_P$ whenever $P' = \alpha(P)$ with α in the Galois group of $\bar{K}$ over K, $\bar{K}$ being the algebraic closure of K. Note that any divisor whose support is contained in the set of K-rational points of $\mathcal{X}$ is a K-divisor. The set of all K-divisors is a subgroup of the group divisor, and it will be denoted by $D_{\mathcal{X}}$.

Remark 3.12. For the sake of simplicity, from now on by the word divisor we will mean a K-rational divisor.

Given a rational function f, it is natural to associate a divisor to f, that is $(f) := \sum v_P(f)P$. Such a divisor is the zero divisor if and only if $f \in K$. For $f \notin K$, (f) can be written as a difference of two effective divisors $(f) = (f)_0 - (f)_\infty$, where $(f)_0 = \sum_{v_P(f)>0} v_P(f)P$ is the zero divisor of f, and $(f)_\infty = \sum_{v_P(f)<0} -v_P(f)P$ is the pole divisor of f.

Example 3.13. Let $\mathcal{X}$ and f be defined as in Example 3.9. Then $(f) = 2P_0 - 2P_\infty$.

Two divisors D and D' are called *linearly equivalent* if $D - D' = (f)$ for a rational function f.

To construct linear codes, the following concept will play a fundamental role. Given a divisor $D = \sum n_p P$, the set of all functions satisfying $v_P(f) \geq -n_P$ at every point P, together with the zero function, is called the *space associated to* D and it is denoted by $L(D)$. For an effective divisor D, $L(D)$ consists of the functions such that all poles lie in $supp(D)$, and the multiplicity of each of them is not greater than n_P. It is straightforward to check that $L(D)$ is a vector space over K, whose dimension is denoted by $l(D)$. We will prove the following lemma:

Lemma 3.14. *Let $D \in D_{\mathcal{X}}$. Then*

1. *if D' is linearly equivalent to D, then $L(D)$ is isomorphic to $L(D')$ (as a vector space over K);*
2. *if $deg(D) < 0$ then $L(D) = \{0\}$;*
3. *$L(0) = K$.*

Proof. (1) As D and D' are equivalent there exists $z \in K(\mathcal{X})$ such that $D = D' + (z)$. Define the mapping $\varphi : L(D) \to K(\mathcal{X})$, $x \mapsto xz$. Clearly, φ is K-linear and its image is contained in $L(D')$: $v_P(xz) = v_P(x) + v_P(z) \geq -n_P + v_P(Z) = -n'_P$ for every $P \in \mathcal{X}$. Moreover, φ is bijective as $\psi : L(D') \to L(D)$, $x \mapsto xz^{-1}$, is an inverse of φ.

(2) Assume there exists $x \in L(D)$, $x \neq 0$. Then $D' := D + (x)$ is effective and linearly equivalent to D. Hence, $0 \leq deg(D') = deg(D)$, which is a contradiction.

(3) Clearly K is contained in $L(0)$. On the other hand, each element in $L(0)$ has no poles, therefore it is a constant.

□

Example 3.15. Consider the curve $\mathcal{X}$ defined over $\mathbf{F}_2$ by $X^3+Y^3+Z^3$. Let $D=2P$, with $P=(0:1:1)\in\mathcal{X}$. We look for elements in $L(D)$, that is rational functions having a pole of multiplicity at most 2 at P, and defined elsewhere. Clearly any constant functions belong to $L(D)$. Let $f=X/(Y+Z)=(Y^2+YZ+Z^2)/X^2$. By Lemma 3.7 $t=X/Z$ is a local parameter at P. Write $f=gt^{-2}$ where $g=(Y^2+YZ+Z^2)/Z^2$. As $g\in O_P\setminus M_P$ we have $v_P(f)=-2$. Note that as f is defined at every point of $\mathcal{X}$ different from P, $f\in L(D)$. As f and 1 are clearly linearly independent over K, the dimension of $L(D)$ is at least 2. We will see later that actually equality holds.

3.3. **The Riemann-Roch Theorem.** The Riemann-Roch Theorem is one of the most famous theorems in Algebraic Geometry. It deals with the computation of $l(D)$, the dimension of the vector space $L(D)$.

Let $\mathcal{X}$ be a curve defined by $F(X,Y,Z)$ and let d be the degree of $\mathcal{X}$. We introduce the value $g=(d-1)(d-2)/2$, which is called the *genus* of $\mathcal{X}$[1]. We also define a canonical divisor as any divisor W such that $deg(W)=2g-2$ and $l(W)=g$.

Theorem 3.16 (Riemann-Roch Theorem)**.** *Given a divisor D,*

$$l(D)=deg(D)+1-g+l(W-D)$$

where W is any canonical divisor.

Calculating $l(W-D)$ is not easy in general. Anyway, as a corollary to the Riemann-Roch Theorem we get that

Corollary 3.17. *For any divisor D such that $deg(D)\geq 2g-1$,*

$$l(D)=deg(D)+1-g$$

Proof. By Riemann-Roch Theorem we have $l(D)=deg(D)+1-g+l(W-D)$, where W is a canonical divisor. As $deg(D)\geq 2g-1$ and $deg(W)=2g-2$, we have $deg(W-A)<0$. By (2) of Lemma 3.14 $l(W-A)=0$, and the claim follows. □

Example 3.18. For q a prime power, let $\mathcal{X}$ be the curve defined by Y over $\mathbf{F}_q$. We keep the notation of Example 3.9. For an integer k, $1\leq k\leq q$, let $D=(k-1)P_\infty$. We will prove that $L(D)$ coincides with the vector space

$$V=\{f(X,Z)/Z^{k-1}\mid f(X,Z)\in\mathbf{F}_q[X,Z],\ \text{homogenous},\ deg(f)\leq k-1\}.$$

[1]The genus of a curve is the most important birational invariant. In the case of non-smooth algebraic curves the definition of genus is much more complicated

First we show that $V \subseteq L(D)$. For $f \in V$, write $f = (a_0Z^{k-1} + a_1XZ^{k-2} + \ldots + a_{k-1}X^{k-1})/Z^k$. Then $f = a_0f_0 + a_1f_1 + \ldots + a_{k-1}f_{k-1}$, where $f_i = (X/Z)^i$. As by Proposition 3.7 f_1^{-1} is a local parameter at P_∞, Proposition 3.8 yields $v_{P_\infty}(f) = -i_0$, where $i_0 = max\{0 \leq i \leq k-1 \mid i \neq 0\}$. Taking into account that f is defined at each point of $\mathcal{X}$ different from P_∞, we have $(f)_\infty = -i_0P_\infty$, and hence $f \in L(D)$. To prove the assertion it is enough to show that $dim(V) = l(D)$. Clearly, $dim(V) = k$. As the genus g of $\mathcal{X}$ is equal to 0, by Corollary 3.17 $l(D) = k$ as well.

Example 3.19. Let $\mathcal{X}$ be as in Example 3.18. Let $P_1 = (a_1 : 0 : 1), \ldots, P_n = (a_n : 0 : 1)$ be n distinct points of $\mathcal{X}$. For $v_1, v_2, \ldots, v_2$ non-zero elements of $\mathbf{F}_q$, let $U \in \mathbf{F}_q[X]$ be such that $deg(U) \leq n-1$ and $U(a_i) = v_i$ for all i, $1 \leq i \leq n$. Write $U = u_0 + u_1X + \ldots + u_{n-1}X^{n-1}$, and u be the rational function on $\mathcal{X}$ defined by $u = (u_0Z^{n-1} + u_1XZ^{n-2} + \ldots + u_{n-1}X^{n-1})/Z^{n-1}$. Now, consider the space $L(D)$, where $D = (k-1)P_\infty - (u)$. We claim that the set

$$uf_0,\ uf_2,\ \ldots,\ uf_{k-1},$$

is a basis of $L(D)$. where $f_i = (X/Z)^i$. From Example 3.18 we know that $(f_i) = iP_0 - iP_\infty$. Hence

$$(uf_i) + D = (u) + (f_i) + ((k-1)P_\infty - (u)) = iP_0 + (k-1-i)P_\infty \geq 0$$

that is $uf_i \in L(D)$ for all i, $0 \leq i \leq k-1$. It is left as an exercise to the reader the proof that the uf_i's are linearly independent. By Corollary 3.17, the dimension of $L(D)$ is equal to k, and hence the assertion is proved.

3.4. **One-point divisors.** In Section 6 we will be concerned with the particular case when $D = mP$, with P a K-rational point of $\mathcal{X}$, $m > 0$. The elements in $L(D)$ are those functions f such that $(f)_\infty = lP$, $l \leq m$. Let $H(P)$ be the following set of non-negative integers:

$$H(P) := \{l|\ \text{there exists } f \in K(\mathcal{X}) \text{ with } (f)_\infty = lP\}.$$

Clearly $H(P)$ is a semigroup, called the *Weierstrass semigroup* at P. The elements in $H(P)$ are called *non-gaps* at P, whereas any integer $s \in \mathbf{N} \setminus H(P)$ is called a *gap*.

Proposition 3.20. *The dimension of $L(mP)$ is equal to the number of non-gaps at P which are less than or equal to m.*

Proof. Note that s is a gap if and only if $L((s-1)P) = L(sP)$. Consider the chain of vector spaces $L(0) \subseteq L(P) \subseteq L(2P) \subseteq \ldots \subseteq L(mP)$. For any i, $0 \leq i \leq m$, the difference $l(iP) - l((i-1)P)$ is at most 1: any two elements f_1, f_2 in $L(iP) \setminus L((i-1)P)$ are linearly dependent over K as f_1/f_2 has no poles and therefore is an element of K. Moreover, by (3) of Lemma 3.14 $dimL(0) = 1$. Hence the proposition is proved. □

By Riemann-Roch Theorem, $L((s-1)P) = L(sP)$ if and only if $l(W-(s-1)P) = l(W-sP)+1$, where W is a canonical divisor. By (2) of Lemma 3.14 this is impossible when $s \geq 2g$. This proves the following proposition.

Proposition 3.21. *Any integer $s \geq 2g$ is a non-gap at every $P \in \mathcal{X}$.*

Moreover, we have that

Proposition 3.22. *There are exactly g gaps at every $P \in \mathcal{X}$.*

Proof. Corollary 3.17 yields that $dim L(2gP) = g+1$. By Proposition 3.20 the number of non-gaps at P which are less than or equal to $2g$ is $g+1$. Hence, by Proposition 3.21 the number of gaps at P is g. □

Corollary 3.23. *If $g \geq 1$ there is at least one gap at every $P \in \mathcal{X}$. As $H(P)$ is a semigroup, 1 is a gap at every $P \in \mathcal{X}$*

The following lemma will be useful in the sequel.

Lemma 3.24. *Let $f_1, \dots f_r \in L(mP)$ be such that $v_P(f_i) \neq v_P(f_j)$ for any $i \neq j$, $1 \leq i, j \leq r$. Then $f_1, \dots, f_r$ are linearly independent over K.*

Proof. Suppose that there exist $\alpha_1, \dots, \alpha_r \in K$ such that $0 = \alpha_1 f_1 + \dots + \alpha_r f_r$. Without loss of generality assume that $\alpha_i \neq 0$ for any $1 \leq j \leq r$. Then by (2) of Proposition 3.8 $v_P(\alpha_1 f_1 + \dots + \alpha_r f_r) = min\{v_P(f_i) \mid 1 \leq i \leq r\}$. Hence $\alpha_1 f_1 + \dots + \alpha_r f_r$ cannot be the 0 function. □

Example 3.25. We keep the notation of example 3.15. As the genus of $\mathcal{X}$ is equal to 1, 1 is the only gap at P. By Proposition 3.20 $l(2P) = 2$.

Example 3.26. Let $\mathcal{X}$ be the Hermitian curve defined over the finite field with q^2 elements (see Example 3.5). Let $P = (0:1:0)$. We claim that for any $m > 0$ a basis of $L(mP)$ is

$$\{(X^i Y^j)/Z^{i+j} \mid iq + j(q+1) \leq m,\ i \geq 0,\ 0 \leq j \leq q-1\}.$$

We first prove that $f_{i,j} = (X^i Y^j)/Z^{i+j}$ belongs to $L(mD)$ when $iq + j(q+1) \leq m,\ i \geq 0,\ 0 \leq j \leq q-1$. Note that the upper bound on j ensures that the $f_{i,j}$'s are pairwise different. As P is the only point of $\mathcal{X}$ with Z-coordinate equal to 0, each $f_{i,j}$ has a pole divisor of type sP. By Proposition 3.7, the function $t = X/Y$ is a local parameter at P. As $t^{q+1} = (Z/Y) + (Z/Y)^q$ we have

$$q+1 = v_P(t^{q+1}) = v_P((Z/Y) + (Z/Y)^q) = v_P(Z/Y)$$

by (2) of Proposition 3.8. Moreover, as $(X/Z)^{q+1} = (Y/Z)^q + (Y/Z)$ we have

$$(q+1)v_P(X/Z) = v_P((Y/Z)^q + (Y/Z)) = -q(q+1)$$

again by (2) of Proposition 3.8. Hence,

$$v_P(f_{i,j}) = -iq - j(q+1) \geq -m,$$

that is $f_{i,j} \in L(mP)$. By Lemma 3.24 the $f_{i,j}$'s are linearly independent over K. It is left as an exercise the proof that $H(P) = \{iq + j(q+1) \mid 0 \leq i, j\}$ [Hint: the genus g of $\mathcal{X}$ is equal to $q(q-1)/2$]. Hence, the number of non-gaps which are less than or equal to m is equal to the number of the $f'_{i,j}s$. By Lemma 3.20 the proof is complete.

Exercise 3.27. Let $\mathcal{X}$ be the curve defined over the finite field with 49 elements by $Y^7Z + YZ^7 - X^8$. Let $P = (0:1:0)$. Find a basis of $L(10P)$, $L(20P)$ and $L(30P)$.

4. Algebraic-Geometric codes

Throughout this section we fix the following notation.

- $\mathcal{X}$ will be a curve defined over $\mathbf{F}_q$.
- $\mathbf{F}_q(\mathcal{X})$ (resp. $D_{\mathcal{X}}$) denotes the field of rational functions (resp. the group of $\mathbf{F}_q$-divisors) of $\mathcal{X}$.
- If $f \in \mathbf{F}_q(\mathcal{X}) \setminus \{0\}$, (f) denotes the divisor associated with f and $(f)_0$ (resp. $(f)_\infty$) denotes the zero (resp. pole) divisor of f.
- For $E \in D_{\mathcal{X}}$, $L(E)$ denotes the $\mathbf{F}_q$-vector space associated with E, i.e.,

$$L(E) = \{f \in \mathbf{F}_q(\mathcal{X}) \setminus \{0\} : E + (f) \geq 0\} \cup \{0\}\,.$$

  We set $\ell(E) := dim(L(E))$.

Let $P_1, \ldots, P_n$ be n distinct $\mathbf{F}_q$-rational points of $\mathcal{X}$ and let $G \in D_{\mathcal{X}}$ such that $v_{P_i}(G) = 0$ for $i = 1, \ldots, n$. Let

$$\begin{aligned} e = e_{P_1,\ldots,P_n} : L(G) &\to \mathbf{F}_q^n \\ f &\mapsto (f(P_1), \ldots, f(P_n))\,, \end{aligned}$$

which is an $\mathbf{F}_q$-linear map. Set $D := P_1 + \ldots + P_n$.

Definition 4.1. The Goppa code associated with D and G is $C_{D,G} := e(L(G))$.

Exercise 4.2. Prove that the Reed-Solomon code in Section 2 is a Goppa code constructed from the curve $\mathcal{X}$ defined by Y, and associated with divisors of type $D = P_1 + \ldots + P_n$ and $G = (k-1)P_\infty$ (cf. Example 3.18).

Exercise 4.3. The Generalized Reed-Solomon code in Section 2 is a Goppa code constructed from the curve $\mathcal{X}$ defined by Y, and associated with divisors of type $D = P_1 + \ldots + P_n$ and $G = (k-1)P_\infty + (u)$ (cf. Example 3.19).

Lemma 4.4. *Let $k := dim(C_{D,G})$ and d be the minimum distance of $C_{D,G}$. Then*

(1) $k = \ell(G) - \ell(G - D)$;
(2) $d \geq n - deg(G)$.

Proof. (1) The map e is surjective from $L(G)$ to $C_{G,D}$. Then, by linear algebra, $k = \ell(G) - dim\mathrm{Ker}(e)$. Since $\mathrm{Ker}(e) = L(G-D)$, (1) follows.

(2) Let $\vec{x} = (f(P_1), \ldots, f(P_n))$ such that $w(\vec{x}) = d$. Then there exist $n-d$ points, say $P_{i_1}, \ldots, P_{i_{n-d}}$, such that $f(P_{i_j}) = 0$, i.e. $v_{P_{i_j}}(f) \geq 1$. Then $f \in L(G - (P_{i_1} + \ldots + P_{i_{n-d}}))$ and hence

$$deg(G) - (n-d) \geq 0\,.$$

Now the claim follows. □

Remark 4.5. Suppose that $n - deg(G) > 0$. Then $d(C_{D,G}) = n - deg(G)$ if and only if there exists $D' \in D_{\mathcal{X}}$ such that $0 \leq D' \leq D$, $deg(D') = deg(G)$, and $dimL(G-D') > 0$. In fact, if $d(C_{D,G}) = n - deg(G)$ then there exists $f \in L(G)$ having exactly $deg(G)$ different zeros in $supp(D)$, say P_{i_j}, $j = 1, \ldots, deg(G)$. Then $D' := \sum_{j=1}^{deg(G)} P_{i_j}$ satisfies all the above conditions. Conversely, supppose there exists $D' \in D_{\mathcal{X}}$ such that $0 \leq D' \leq D$, $deg(D') = deg(G)$, and $dimL(G-D') > 0$. Let $f \in L(G-D')$. Then $(f) = D' - G$ and so there is an element of $C_{D,G}$ of weight $n - deg(G)$.

Proposition 4.6. *Let $C_{D,G}$ be a Goppa code with parameters k and d as above. Let g be the genus of the underlying curve.*

(1) *If $n > deg(G)$, then $k = \ell(G)$. In particular, $k \geq deg(G) + 1 - g$ and so $d + k \geq n + 1 - g$. Furthermore, a generator matrix of $C_{D,G}$ is given by*

$$M := \begin{pmatrix} f_1(P_1) & \ldots & f_1(P_n) \\ \vdots & \vdots & \vdots \\ f_k(P_1) & \ldots & f_k(P_n) \end{pmatrix},$$

where $f_1, \ldots, f_k$ is an $\mathbf{F}_q$-basis of $L(G)$.

(2) *If $n > deg(G) > 2g - 2$, then $k = deg(G) + 1 - g$.*

Proof. (1) We have that $L(D-G) = 0$ and hence the first part of (1) follows from Lemma 4.4(1) and the Riemann-Roch theorem. To see that M is a generator matrix of $C_{D,G}$ we have to show that the rows $\vec{x}_1, \ldots, \vec{x}_k$ of M are $\mathbf{F}_q$-linearly independent. Suppose that $\sum_{i=1} a_i \vec{x}_i = \vec{o}$ with $a_i \in \mathbf{F}_q$. Then $\sum_{i=1}^{k} a_i f_i(P_j) = 0$ for $j = 1, \ldots, n$. Then $\sum_{i=1}^{k} a_i f_i \in L(G-D)$ and so $a_i = 0$ for each i. This completes the proof of (1).

(2) The claim follows from (1) and Corollary 3.17. □

Remark 4.7. The Singleton bound (Corollary 1.13) together with (1) of Proposition 4.6 for a code $C = C_{D,G}$ with $n > deg(G)$ yield

$$n + 1 - g \leq d + k \leq n + 1\,.$$

In particular, if the underlying curve has genus 0, then C is MDS. This proves also that Generalized Reed-Solomon codes are MDS codes.

Remark 4.8. It is, in general, a very hard problem to obtain lower bounds for the minimum distance of a given code (or a given class of codes). One of the reasons for the interest in AG-codes is that for this large class of codes a good lower bound for the minimum distance is available (see Proposition 4.6).

We state an important result on Goppa codes, whose proof is beyond the purposes of these notes.

Proposition 4.9. *Let $\mathcal{X}$, $D = P_1 + \ldots + P_n$ and G be as above. Then there exists a canonical divisor W such that*

$$C_{D,G}^{\perp} = C_{D,D-G+W}\,.$$

5. Bounds on linear codes

A rough gauge of the quality of a linear code C is provided by two invariants: the *transmission rate* $R(C) := k/n$ and the *relative distance* $\delta(C) := d/n$, where n is the length of C, k is its dimension and d its minimum distance. In essence, the purpose of coding theory is to find codes that optimize these invariants.

Let $U_q^{lin} \subset [0,1]^2$ be the set of limit points of all pairs $(\delta(C), R(C))$ coming from linear codes. The region U_q^{lin} is called the *domain* of codes. It is bounded in the unit square by the sides of the unit squares on the axis and by the graph of a continuous function $\alpha_q^{lin} : [0,1] \to [0,1]$ defined by

$$\alpha_q^{lin}(\delta) = \sup\{R : (\delta, R) \in U_q^{lin}\}.$$

For $0 < \delta < (q-1)/q$, the exact value of $\alpha_q^{lin}(\delta)$ is unknown. However, several upper and lower bounds are available.

The *q-ary entropy function* $H_q : [0, (q-1)/q] \to \mathbf{R}$ is defined by $H_q(0) = 0$ and $H_q(x) = x\log_q(q-1) - x\log_q(x) - (1-x)\log_q(1-x)$ for $0 \le x \le (q-1)/q$.

Proposition 5.1. (a) *(Plotkin Bound) For $0 \le \delta \le (q-1)/q$,*

$$\alpha_q(\delta) \le 1 - \frac{q}{q-1}\delta\,.$$

(a) *(Hamming Bound) For $0 \le \delta \le 1$,*

$$\alpha_q(\delta) \le 1 - H_q\left(\frac{\delta}{2}\right)\,.$$

(c) *(Gilbert-Varshamov Bound) For $0 \le \delta \le (q-1)/q$,*

$$\alpha_q(\delta) \ge 1 - H_q(\delta)\,.$$

Remark 5.2. There exists some others much more complicated to upper bounds on $\alpha_q(\delta)$. We mention here the Bassalygo-Elias Bound and the Mc-Eliece-Rodemich-Rumsey-Welch Bound, which are better than both Hamming and Plotkin bounds.

For a long time coding theorists were unable to construct explicit sequences of codes with limit points on or above the Gilbert-Varshamov bound and they were led to suspect that $\alpha_q(\delta) = 1 - H_q(\delta)$ for $0 \leq \delta \leq (q-1)/q$.

Now we consider AG Codes, keeping the notation of the previous section. If we fix the ratio $deg(G)/n$ then the transmission rate $R(C_{D,G})$ increases with the ratio n/g. Therefore to obtain good codes one has to construct curves with as many rational points as possible. Given a curve $\mathcal{X}$ over $\mathbf{F}_q$, let $N(\mathcal{X})$ denote the number of $\mathbf{F}_q$-rational points of $\mathcal{X}$. Note that if $\mathcal{X}_l$ is a sequence of curves defined over $\mathbf{F}_q$ such that their genera g_l tend to ∞ and such that $\lim_{l\to+\infty} \frac{N(\mathcal{X}_l)}{g_l}$ is a positive real number γ, then the part of the line $\delta + R = (\gamma-1)/\gamma$ in the positive quadrant is contained in the domain U_q^{lin}. This follows by taking divisors G_l of degree r_l with $2g_l - 1 \leq r_l < N(\mathcal{X}_l)$, and taking as D the set of all rational points of $\mathcal{X}_l$. Then (1) of Proposition 4.6 tells us that for the code C_{D_l,G_l} we have

$$R_l + \delta_l \geq 1 + (1 - g_l)/N(\mathcal{X}_l)$$

which tends to $(\gamma-1)/\gamma$. Hence this sequence of codes has a limit point on or above the line $\delta + R = (\gamma-1)/\gamma$. The fact that for q a square there exists a sequence of curves $\mathcal{X}_l$ defined over $\mathbf{F}_q$ of genus g_l with the ratio $N(\mathcal{X}_l)/g_l$ tending to $\sqrt{q} - 1$ was observed by Ihara and independently by Tsfasman, Vladut and Zink. For $q \geq 49$ the line $\delta + R = \frac{\sqrt{q}-2}{\sqrt{q}-1}$ comes above the Gilbert-Varshamov bound, and this came at that time as quite as a surprise for coding theorists. Later on, Drinfeld and Vladut generalized the idea of Ihara and Tsfasman, Vladut and Zink by using all prime powers, not just squares. Let $N_q(g)$ be the maximum value of $N(\mathcal{X})$ where $\mathcal{X}$ runs through all curves of genus g defined over $\mathbf{F}_q$. Moreover, we define

$$A(q) := \limsup_{g\to+\infty} \frac{N_q(g)}{g}.$$

By repeating the argument above, it can be proved that the part of the line $\delta + R = (A(q)-1)/A(q)$ in the positive quadrant is contained in the domain U_q^{lin}. The results of Drinfeld and Vladut says that $A(q) \leq \sqrt{q} - 1$. Unfortunately this bound is an upper bound for $A(q)$. At present times, a large amount of research is being performed on the problem of determining bounds on $N_q(g)$ and $A(q)$.

6. One-point Goppa Codes

In this section we deal with a lower bound on the minimum distance of the duals of Goppa codes $C_{D,G}$ where $G = \gamma P$, and P is an $\mathbf{F}_q$-rational point of the underlying curve (see [13, Sec. 4]). Note that $L(G) = L(\tilde{\gamma}P)$, where $\tilde{\gamma}$ is the biggest non-gap at P less than or equal to γ. Hence, we assume that γ is a non-gap at P.

We set

$$H(P) = \{\rho_1 = 0 < \rho_2 < \ldots\},$$

and

$$E_\ell := C_{D,\rho_\ell P}\,, \qquad\qquad C_\ell := E_\ell^\perp\,.$$

Let $\nu_\ell := \#\{(i,j) \in \mathbf{N}^2 : \rho_i + \rho_j = \rho_{\ell+1}\}$.

Definition 6.1. The number

$$d_{\mathrm{ORD}}(\ell) := \min\{\nu_m : m \geq \ell\}$$

is called the *order bound* or the *Feng-Rao designed minimum distance* of C_ℓ.

Let c be the *conductor* of $H(P)$, i.e. c is the largest element $m \in H(P)$ such that $m-1 \notin H(P)$.

Theorem 6.2. $d(C_\ell) \geq d_{\mathrm{ORD}}(\ell)$.

Proof. Let $f_i \in \mathbf{F}_q(X)$ such that $(f_i)_\infty = \rho_i P$. Then $\{f_1, \ldots, f_\ell\}$ is an $\mathbf{F}_q$-basis of $L(\rho_\ell P)$. Let $\vec{h}_i := e(f_i) = (f_i(P_1), \ldots, f_i(P_n))$. Then E_ℓ is generated by $\vec{h}_1, \ldots, \vec{h}_\ell$ and so

$$C_\ell = \{\vec{x} \in \mathbf{F}_q^n : \langle \vec{x}, \vec{h}_i \rangle = 0 \text{ for } i = 1, \ldots, \ell\}\,.$$

Note that there exists N such that for $\ell \geq N$, $E_\ell = \mathbf{F}_q^n$. For $\vec{y} \in \mathbf{F}_q^n$, and for $i, j = 1, \ldots, N$, set

$$s_i(\vec{y}) := \langle \vec{y}, \vec{h}_i \rangle \qquad \text{and} \qquad s_{ij}(\vec{y}) := \langle \vec{y}, \vec{h}_i * \vec{h}_j \rangle\,,$$

where for $\vec{z} = (z_1, \ldots, z_n)$ and $\vec{w} = (w_1, \ldots, w_n)$, $\vec{z} * \vec{w} := (z_1 w_1, \ldots, z_n w_n)$. We have the following $N \times N$ matrix

$$\mathbf{S}(\vec{y}) := (s_{ij}(\vec{y}))\,.$$

Claim 6.3. ([13, Lemma 4.7]) *For $\vec{y} \in \mathbf{F}_q^n$, $w(\vec{y}) = \mathrm{rank}(\mathbf{S}(\vec{y}))$.*

Proof. (*Claim 6.3*) It is easy to see that $\mathbf{S}(\vec{y}) = HD(\vec{y})H^t$, where H is the $N \times n$ matrix with $\vec{h}_i$ as its ith, and $D(\vec{y})$ is the $n \times n$ diagonal matrix with $\vec{y}$ on the diagonal. Since $E_N = \mathbf{F}_q^n$, both H and H^t have rank n and so $\mathrm{rank}(\mathbf{S}(\vec{y})) = \mathrm{rank}(D(\vec{y})) = w(\vec{y})$. □

Claim 6.4. ([13, Lemma 4.9])

(1) *If $\vec{y} \in C_\ell$ and $\rho_i + \rho_j \leq \rho_\ell$, then $s_{ij}(\vec{y}) = 0$;*
(2) *If $\vec{y} \in C_\ell \setminus C_{\ell+1}$ and $\rho_i + \rho_j = \rho_{\ell+1}$, then $s_{ij}(\vec{y}) \neq 0$.*

Proof. (*Claim 6.4*) (1) From $\rho_i + \rho_j \leq \rho_\ell$ we have that $f_i f_j \in L(\rho_\ell P)$, and thus $\vec{h}_i * \vec{h}_j \in E_\ell = C_\ell^\perp$. Then (1) follows.

(2) From $\rho_i + \rho_j = \rho_{\ell+1}$ it follows that $f_i f_j \in L(\rho_{\ell+1}P) \setminus L(\rho_\ell P)$. Then $f_i f_j = \sum_{k=1}^{\ell+1} a_k f_k$ with $a_k \in \mathbf{F}_q$ and $a_{\ell+1} \neq 0$. Thus, $\vec{h}_i * \vec{h}_j = \sum_{k=1}^{\ell+1} a_k \vec{h}_k$ and so $s_{ij}(\vec{y}) = a_{\ell+1}\langle \vec{y}, \vec{h}_{\ell+1} \rangle$ which is not zero as $\vec{y} \notin C_{\ell+1}$. □

Claim 6.5. ([13, Lemma 4.10]) *Let $(i_1, j_1), \ldots, (i_{\nu_\ell}, j_{\nu_\ell})$ be an enumeration of the elements of $\{(i,j) \in \mathbf{N}^2 : \rho_i + \rho_j = \rho_{\ell+1}\}$ in increasing order with respect to the lexicographic order on $\mathbf{N}^2$. Then*

(1) $i_1 < \ldots < i_{\nu_\ell}$ *and* $j_1 > \ldots > j_{\nu_\ell}$;
(2) *For* $\vec{y} \in C_\ell \setminus C_{\ell+1}$, $s_{i_h,j_h}(\vec{y}) \neq 0$ *for* $h = 1, \ldots, \nu_\ell$.

Proof. (*Claim 6.5*) (1) Suppose that $i_u = i_{u+1}$. Then $j_u < j_{u+1}$ and so $\rho_{\ell+1} = \rho_{i_{u+1}} + \rho_{j_{u+1}} > \rho_{i_u} + \rho_{j_u} = \rho_{\ell+1}$, a contradiction. Now suppose that $j_{u+1} \geq j_u$. Then $\rho_{\ell+1} = \rho_{i_{u+1}} + \rho_{j_{u+1}} > \rho_{i_u} + \rho_{j_u} = \rho_{\ell+1}$, which is again a contradiction.

(2) It follows from Claim 6.4(2) since $\rho_{i_h} + \rho_{j_h} = \rho_{\ell+1}$. □

Now, by using the notations above, for $\vec{y} \in C_\ell$, $h = 1, \ldots, \nu_\ell$ and $1 \leq j < j_h$ we have that $s_{i_h,j}(\vec{y}) = 0$. Then for $\vec{y} \notin C_{\ell+1}$ the i_1th, ...,i_{ν_ℓ}th rows of $\mathbf{S}(\vec{y})$ are $\mathbf{F}_q$-linearly independent. Therefore, $\mathrm{rank}(\mathbf{S}(\vec{y})) \geq \nu_\ell$ and from Claim 6.3 we have that

$$d(C_\ell) \geq \min\{\nu_m : m \geq \ell, C_m \supsetneq C_{m+1}\}$$

and the assertion follows.

Theorem 6.6. $d_{\mathrm{ORD}}(\ell) \geq \ell + 1 - g$ *and equality holds if* $\ell \geq 2c - g - 1$.

□

Proof. First we prove a claim.

Claim 6.7. ([13, Thm 5.24], [22, Lemma 3.4(1)]) *Let* $\mu_\ell := \#\{i \mid 1 \leq i \leq \rho_{\ell+1}$ *and* $i, \rho_{\ell+1} - i \notin H(P)\}$. *Then*

$$\nu_\ell = 2\ell + 1 - \rho_{\ell+1} + \mu_\ell \,.$$

Proof. (*Claim 6.7*) We have that

$$\{(i,j) \in \mathbf{N}^2 : \rho_i + \rho_j = \rho_\ell\} = \{(a,b) \in \mathbf{N}_0^2 : a + b = \rho_{\ell+1}\} \setminus (\mathcal{A} \cup \mathcal{B}) \,,$$

where $\mathcal{A} := \{(a,b) \in \mathbf{N}_0^2 : a + b = \rho_{\ell+1}, a \notin H(P)\}$ and $\mathcal{B} = \{(a,b) \in \mathbf{N}_0^2 : a + b = \rho_{\ell+1}, b \notin H(P)\}$. Clearly $\#\mathcal{A} = \#\mathcal{B}$ and this number is equal to $\rho_{\ell+1} - \ell$. Then $\nu_\ell = (\rho_{\ell+1} + 1) - 2(\rho_{\ell+1} - \ell) + \#\mathcal{A} \cap \mathcal{B}$. Since

$$(i,j) \in \mathcal{A} \cap \mathcal{B} \Leftrightarrow 0 < i < \rho_{\ell+1}, i, j = \rho_\ell - i \notin H(P) \,,$$

the statement follows. □

Then we have that $\nu_\ell \geq 2\ell + 1 - \rho_{\ell+1}$. Since $g \geq \rho_{\ell+1} - \ell$, we have $\nu_\ell \geq \ell + 1 - g$ and so $d_{\mathrm{ORD}}(\ell) \geq \ell + 1 - g$. On the other hand, $\rho_{\ell+1} = g + \ell$ for $\ell \geq c - g$ and if $a, b \notin H(P)$, $a + b \leq 2c - 2$. Hence, for $\ell \geq 2c - g - 1$, $\mu_\ell = 0$ and $\nu_\ell = \ell + 1 - g$. This completes the proof of Theorem 6.6. □

7. MDS codes and Almost MDS codes

In this section a linear code C over $\mathbf{F}_q$ with length n, dimension k and minimum distance k will be called an $[n, k, d]$-code. In Section 1 we defined MDS codes as those linear codes which meet the Singleton bound (see Corollary 1.13). That is, MDS codes have have the best error-correcting capability, for given length and dimension. The following is a natural definition in this context.

Definition 7.1. The Singleton defect of an $[n, k, d]$-code C is $s(C) = n - k + 1 - d$.

An MDS code is a code with Singleton defect equal to 0. When $s(C) = 1$, C is said to be an Almost MDS code (AMDS code for short).

Remark 7.2. By Remark 4.7 for an AG-code $C = C_{D,G}$ with $n > deg(G)$ the Singleton defect $s(C)$ is less than or equal to the genus g of the underlying curve.

As a corollary to Lemma 1.12 we can state a very simple but useful connection between coding theory and finite geometry. Let $PG(r, q)$ be the projective space of r dimensions over $\mathbf{F}_q$. A set of m points in $PG(r, q)$ are said to be in *general position* if they are not contained in a subspace of dimension $m - 2$.

Definition 7.3. A subset K of n points in $PG(r, q)$ is said to be an *n-set of kind e* if $e + 1$ points in K are always in general position, but some $e + 2$ of them are not.

Proposition 7.4. *The following are equivalent:*

(1) *C is an $[n, k, d]$-code.*
(2) *The columns of the parity check matrix of C are the homogenous coordinates of the points of an n-set of kind $d - 1$ in $PG(n - k - 1, q)$.*

Proof. The claim follows from Lemma 1.12. □

An *n-arc* in $PG(r, q)$ is an n-set of kind r. An *n-track* in $PG(r, q)$ is an n-set of kind $r - 1$. By the above proposition, MDS (resp. AMDS) $[n, k, d]$-codes over $\mathbf{F}_q$, and n-arcs (resp. n-tracks) in $PG(n - k - 1, q)$ are equivalent objects.

7.1. **MDS codes.** Two of the main problems on MDS codes are the following: (a) finding the maximum length of an MDS code of a given dimension, (b) characterizing the codes having this maximum length. In this section, these problems will be approached from a geometric point of view, i.e. in terms of arcs in projective spaces.

By Propositions 1.15 and 7.4, the maximum lenght of an MDS code over $\mathbf{F}_q$ of dimension $s + 1$ is equal to the maximum size of an n-arc in $PG(s, q)$, denoted by $m(s, q)$. The following conjecture is known as the *main conjecture on MDS codes*:

Conjecture 7.5.

$$m(s,q) = \begin{cases} s+2 & \text{if } s \geq q-1, \\ q+2 & \text{if } q \text{ is even and } s \in \{2, q-2\}, \\ q+1 & \text{in all other cases.} \end{cases}$$

7.1.1. *MDS codes of dimension* 3. The main conjecture on MDS codes has been proved for $s = 2$, that is for MDS codes of dimension 3. This is a classical result in finite geometry, going back to the 50's.

An $m(2,q)$-arc in $PG(2,q)$, q odd, is called an *oval* and an $m(2,q)$-arc in $PG(2,q)$, q even, is called a *hyperoval*.

Theorem 7.6 (Segre)**.** *For q odd, an oval is the set of rational points of a conic.*

Bose showed that, for q even, a conic plus its nucleus (the intersection point of its tangents) is a hyperoval. A hyperoval of this type is called *regular*. As shown by Segre, for $q = 2, 4, 8$, every hyperoval is regular. For $q = 2^h$, $h \geq 4$, there exist *irregular* hyperovals, that is, hyperovals which are not the union of a conic and its nucleus. Several infinite classes of irregular hyperovals are known. The problem of classifying hyperovals would appear to be difficult.

Finding the values of n for which an n-arc is always contained in an oval, for q odd, or hyperoval, for q even, is relevant for solving problems in higher-dimensional spaces.

Let $m'(2,q)$ denote the second largest size that a complete arc in $PG(2,q)$ can have. Segre showed that

$$m'(2,q) \leq \begin{cases} q - \frac{1}{4}\sqrt{q} + \frac{7}{4} & \text{if } q \text{ is odd,} \\ q - \sqrt{q} + 1 & \text{otherwise.} \end{cases} \tag{7.1}$$

Besides small q, namely $q \leq 29$, the only case where $m'(2,q)$ has been determined is for q an even square. Indeed, for q square, examples of complete $(q - \sqrt{q} + 1)$-arcs show that

$$m'(2,q) \geq q - \sqrt{q} + 1\,, \tag{7.2}$$

and so the bound (7.1) for an even q square is sharp. This result has been recently extended by Hirschfeld and Korchmáros who showed that the third largest size that a complete arc can have is upper bounded by $q - 2\sqrt{q} + 6$.

If q is not a square, Segre's bounds were notably improved by Voloch.

If q is odd, Segre's bound was slightly improved to $m'(2,q) \leq q - \sqrt{q}/4 + 25/16$ by Thas. If q is an odd square and large enough, Hirschfeld and Korchmáros significantly improved the bound to

$$m'(2,q) \leq q - \frac{1}{2}\sqrt{q} + \frac{5}{2}\,. \tag{7.3}$$

The two last bounds suggest the following problem, which seems to be difficult and has remained open since the 60's.

Problem 7.7. For q an odd square, is it true that $m'(2,q) = q - \sqrt{q} + 1$?

The answer is negative for $q = 9$ and affirmative for $q = 25$. So Problem 7.7 is indeed open for $q \geq 49$.

All cited bounds on $m'(2,q)$ are proved in a similar way. Segre associates to an n-arc in $PG(2,q)$ a plane curve $\mathcal{C}$ in the dual plane of $PG(2,\bar{\mathbf{F}}_q)$, where $\bar{\mathbf{F}}_q$ denotes the algebraic closure of $\mathbf{F}_q$. This curve is defined over $\mathbf{F}_q$ and it is called *the envelope of* the arc. For $P \in PG(2,\bar{\mathbf{F}}_q)$, let ℓ_P denote the corresponding line in the dual plane. The following result summarizes the main properties of $\mathcal{C}$ for the odd case.

Theorem 7.8. *Let $\mathcal{K}$ be an n-arc in $PG(2,q)$. If q is odd, then the following statements hold:*

(1) *The degree of $\mathcal{C}$ is $2t$, with $t = q - n + 2$ being the number of 1-secants through a point of $\mathcal{K}$.*
(2) *All nt of the 1-secants of $\mathcal{K}$ belong to $\mathcal{C}$.*
(3) *Each 1-secant ℓ of $\mathcal{K}$ through a point $P \in \mathcal{K}$ is counted twice in the intersection of $\mathcal{C}$ with ℓ_P.*
(4) *The curve $\mathcal{C}$ contains no 2-secant of $\mathcal{K}$.*
(5) *The irreducible components of $\mathcal{C}$ have multiplicity at most two, and $\mathcal{C}$ has at least one component of multiplicity one.*
(6) *For $n > (2q+4)/3$, the arc $\mathcal{K}$ is incomplete if and only if $\mathcal{C}$ admits a linear component over $\mathbf{F}_q$. For $n > (3q+5)/4$, the arc $\mathcal{K}$ is a conic if and only it is complete and $\mathcal{C}$ admits a quadratic component over $\mathbf{F}_q$.*

Proof. The proof of this theorem can be found in [11], and is based on the classical Theorem of Menelaus. □

The common idea of the proofs of the bounds on $m'(2,q)$ is that $\mathcal{C}$ has a lot of points, namely at least nt, is defined over $\mathbf{F}_q$, and its degree $2t$ is not too big. Then a good upper bound on the number of $\mathbf{F}_q$-rational points of a curve, for example Hasse-Weil Theorem, or the theorem of Stöhr and Voloch, is used to show that for n big enough $\mathcal{C}$ is a union of pencils. The vertices of these pencils are points which extend the original arc to an oval.

7.1.2. *MDS codes of dimension greater than* 3. Again, the main question is to find an upper bound for the size of an n-arc in $PG(s,q)$, with $s \geq 3$. The situation is essentially different if s is small or large compared to q. Let us first consider the case s small in detail.

Definition 7.9. A *normal rational curve* of $PG(s,q)$ is a subset of points which is projectively equivalent to

$$\{(1,t,t^2,\ldots,t^s) \mid t \in \mathbf{F}_q\} \cup \{(0,0,\ldots,0,1)\}.$$

Note that a normal rational curve of $PG(2,q)$ is a conic. It is very easy to see that a normal rational curve of $PG(s,q)$ is indeed a $(q+1)$-arc. Let $m'(s,q)$ denote the size of the second largest complete arc in $PG(s,q)$.

Theorem 7.10 (Kaneta-Maruta)**.** *If every $(q+1)$-arc of $PG(s,q)$ is a normal rational curve, then $q+1$ is the maximum value of n for which n-arcs exist in $PG(s+1,q)$. If in addition $m'(s,q) < q$, then any $(q+1)$-arc in $PG(s+1,q)$ is a normal rational curve.*

Outline of the proof. Take a $(q+2)$-arc $\mathcal{K}$ in $PG(s+1,q)$ and project it from its points $r_i \in \mathcal{K}$ onto hyperplanes α_i such that $r_i \notin \alpha_i$. Then we get a normal rational curve $\mathcal{K}_i$ in each hyperplane α_i, and $\mathcal{K}$ is contained in the intersection of the cones with vertex r_i and base $\mathcal{K}_i$. As the intersection of these cones is a normal rational curve, we have that $\mathcal{K}$ has at most $q+1$ points, a contradiction. Hence $m(s+1,q) = q+1$. The second assertion can be proved similarly. In fact, each projection K_i of a $(q+1)$-arc is contained in a normal rational curve, as the size of K_i is q and $m'(s,q) < q$. □

For q odd, Segre's Theorem 7.6 is a good starting point for the application of Theorem 7.10. More precisely, it gives $m(s,q) = q+1$ for $s = 3$. Taking into account (7.1), we have that any $(q+1)$-arc in $PG(3,q)$ is a normal rational curve. These results can be extended to higher dimensions by induction. Roughly speaking, from the projection argument one can suspect that we lose one when the dimension is increased by one, hence the importance of improving on the difference between q and $m'(2,q)$. More precisely, the following result holds true.

Theorem 7.11. *Let q be odd.*

(a) $m(s,q) = q+1$, *if* $s < q+4-m'(2,q)$,
(b) *any $(q+1)$-arc in $PG(s,q)$ is a normal rational curve if* $s < q+3-m'(2,q)$.

The theorem was first proved by Thas, the improvement between the bounds in (b) and (a) is due to Kaneta and Maruta.

It is worthwhile to mention that in $PG(4,9)$ there are two different types of $(q+1)$-arcs. Of course we have the normal rational curves and the second type is the set

$$\{(1,x,x^2+\sigma x^6,x^3,x^4)\} \cup \{(0,0,0,0,1)\}$$

where σ is a non-square of $\mathbf{F}_9$.

The case q even is more complicated as we cannot start from 3 dimensions. However, already in three dimensions, Casse and Glynn could characterize $(q+1)$-arcs.

Theorem 7.12. *In $PG(3,q)$ with $q = 2^h$ every $(q+1)$-arc is projectively equivalent to the set*

$$\{1,t,t^{2^r},t^{2^r+1}\} \cup \{(0,0,0,1)\}$$

for some r with $(r,h) = 1$.

Then in four dimensions the same authors proved even more.

Theorem 7.13. *Any $(q+1)$-arc of $PG(4,q)$, $q \geq 8$ even, is a normal rational curve.*

The difficulty in extending the result s in higher dimensions was that there was no reasonable estimate available on $m'(3,q)$ at that time. This very important step was first done in a paper by Bruen, Thas and Blokhuis in 1988. However, this is not yet enough to apply induction. Currently, the best bounds for $m(s,q)$ and $m'(s,q)$ are due to Storme and Thas (1993).

Theorem 7.14. *Let q be even.*

(a) *In $PG(s,q)$, $s \geq 4$ and $q > (2s - \frac{11}{2})^2$, we have $m(s,q) = q+1$.*
(b) *In $PG(s,q)$, $s \geq 4$ and $q > (2s - \frac{7}{2})^2$, every $(q+1)$-arc is a normal rational curve.*
(c) *In $PG(s,q)$, $s \geq 4$ and $q > (2s - \frac{7}{2})^2$, we have $m'(n,q) \leq q - \frac{\sqrt{q}}{2} + s - \frac{3}{4}$.*

Finally, there is a relatively easy case, when the dimension os bigger than q. Of course, we always have an arc consisting of $(s+1)$ points (the points of the fundamental simplex), and it is not too difficult to see that other points cannot be added to this set.

7.2. **Almost MDS codes.** The interest in AMDS codes comes from the possibility to construct AMDS codes with length bigger than $q+1$. Let $\mu(s,q)$ be the maximum length n for which there exists an $[n, n-s-1, s+1]$-code over $\mathbf{F}_q$, that is the maximum size of an n-track in $PG(s,q)$.

AMDS codes over $\mathbf{F}_q$ of length bigger than $q+1$ arise from elliptic curves (i.e. curves of genus $g=1$) via Goppa construction. In particular, An AMDS code over $\mathbf{F}_q$ of length n and dimension k exists for every n and $k = 2, 3, \ldots, n$, provided that some elliptic curve over $\mathbf{F}_q$ has exactly $n+1$ $\mathbf{F}_q$-rational points. Roughly speaking, this follows from Remark 7.2.

However, we describe in detail AMDS codes arising from elliptic curves, in order to study their extendibility.

Let $\mathcal{E}$ be an elliptic plane curve defined over $\mathbf{F}_q$ with affine equation

$$f(X,Y) := Y^2Z + a_1XYZ + a_2YZ^2 - X^3 - a_3X^2Z - a_4XZ^2 - a_5Z^3 = 0\,,$$

where $a_i \in \mathbf{F}_q$ for $i = 1, \ldots, 5$.

Remark 7.15. It can be proved that any plane elliptic curve defined over $\mathbf{F}_q$ and with at least one $\mathbf{F}_q$-rational point of inflection is projectively equivalent to a curve of the above form.

Let $n+1 := \#\mathcal{E}(\mathbf{F}_q)$, the number of $\mathbf{F}_q$-rational points of $\mathcal{E}$. Then $\mathcal{E}(\mathbf{F}_q)$ consists of n affine points, say $P_1, \ldots, P_n$, together with the infinite point $P_{n+1} = P_\infty = (0:0:1)$.

Let $\Sigma = K(\mathcal{E})$ be the rational function field of $\mathcal{E}$. Let also x be the rational function represented by X/Z, and y the one represented by Y/Z. It is easy to see that the number of zeros of x is 2, whereas the number of zeros of y is 3. By Theorem 3.11 we have $v_{P_\infty}(x) = -2$ and $v_{P_\infty}(y) = -3$.

For any integer $i > 1$, let

$$\psi_i(X,Y) := \begin{cases} Y^s & \text{if } i = 3s,\ s \geq 1\,, \\ XY^s & \text{if } i = 3s+2,\ s \geq 0\,, \\ X^2Y^s & \text{if } i = 3s+4,\ s \geq 0\,. \end{cases}$$

Note that $v_{P_\infty}(\psi_i(x,y)) = -i$ and that $\psi_i(x,y)$ is defined at every point of $\mathcal{E}$ different from P_∞. Let us fix an integer $k \in \{3,4,\ldots,n\}$. For any $i \in \{2,\ldots,k\}$, the rational function $\psi_i(x,y)$ belongs to $L(kP_\infty)$. By Corollary 3.17, $1, \psi_2(x,y), \ldots, \psi_k(x,y)$ is a basis of $L(kP_\infty)$.

Then by Proposition 4.6 the AG code $C_k := C_{D,G}$ with $G := kP_\infty$, $D := P_1 + \ldots + P_n$ has length n, dimension k, and by Lemma 4.4 its minimum distance is at least $n-k$.

For every prime power q, the above codes C_k provides AMDS codes of length up to $N_q(1) - 1$, where $N_q(1)$ denotes the maximum number of $\mathbf{F}_q$-rational points that an elliptic curve defined over $\mathbf{F}_q$ can have. From work by Waterhouse (see e.g. [27, Thm. 2.3.17]), we know that for every $q = p^r$, p prime,

$$N_q(1) = \begin{cases} q + \lceil 2\sqrt{q} \rceil, & \text{for } p \mid \lceil 2\sqrt{q} \rceil \text{ and odd } r \geq 3, \\ q + \lceil 2\sqrt{q} \rceil + 1, & \text{otherwise,} \end{cases}$$

where $\lceil x \rceil$ is the integer part of x.

Actually, a little bit more can be done to obtain longer AMDS codes. Let $G_k(\mathcal{E})$ be the $(k \times n)$ matrix whose j^{th}-column is the k-tuple $(1, \psi_2(P_j), \psi_3(P_j), \ldots \psi_k(P_j))$ for $j = 1, \ldots, n$. Of course, $G_k(\mathcal{E})$ is a generator matrix for C_k. It can be proved that if the column $(0,0,0,\ldots,0,1)$ is added, then the resulting matrix is a generator matrix of an AMDS code of length $n+1$ and dimension k. This code we will referred to as a k-elliptic code. Constructing $[n,k,d]$ NMDS codes over $\mathbf{F}_q$ of length bigger than $N_q(1)$ appears to be hard for $q \geq 17$ and $k > 3$.

In this context the following definition turns out to be useful.

Definition 7.16. An $[n,k,d]$ code C over $\mathbf{F}_q$ is *h-extendable* if there exists an $[n+h,k,d+h]$ code over $\mathbf{F}_q$ C' such that $\pi_{n,h}(C') = C$, where $\pi_{n,h} : \mathbf{F}_q^{n+h} \to \mathbf{F}_q^n$, $\pi_n(a_1,\ldots,a_{n+h}) = (a_1,\ldots,a_n)$. A 1-extendable code is simply referred to as extendable code.

The following is a very recent result [7].

Theorem 7.17. *Let $q \geq 121$ be an odd prime power. Let $\mathcal{E}$ be an elliptic curve defined over $\mathbf{F}_q$ whose j-invariant $j(\mathcal{E})$ is different from 0. Then,*

(1) *for $k = 3, 6$, the k-elliptic code associated to $\mathcal{E}$ is non-extendable;*
(2) *for $k = 4$, any k-elliptic code associated to $\mathcal{E}$ the not 2-extendable;*
(3) *for $k = 5$, any k-elliptic code associated to $\mathcal{E}$ the not 3-extendable.*

7.3. **Near MDS codes.** Unlike the MDS case, the dual of an AMDS code need not to be AMDS. To distinguish this property we define an AMDS code such that its dual is AMDS to be a Near MDS code (NMDS for short). Actually, the k-elliptic codes defined in Section 7.2 are Near MDS.

It can be easily proved that an $[n, k, d]$ NMDS code can be viewed as an n-track $\mathcal{K}$ in $PG(k-1, q)$, with the additional property that every $k+1$ points from $\mathcal{K}$ are in general position. If $k = 3$, these properties reduce to (a) there exists three collinear points in $\mathcal{K}$, (b) no four points from $\mathcal{K}$ lie on a line. In the notation of finite geometry an n-set in $PG(2, q)$ satisfying (a) and (b) is said to be an $(n, 3)$-arc. Hence, the maximum size of an $(n, 3)$-arc in $PG(2, q)$, denoted by $m(3, q)$, is equal to the maximum length of an NMDS code of dimension 3 over $\mathbf{F}_q$. Computing the exact value of $m(3, q)$ seems to be very difficult. Some results have been obtained for small values of q by Ball ([1]) and very recently by Marcugini, Milani and Pambianco ([20], [21]).

q	4	5	7	8	9	11	13
$m(3, q)$	9	11	15	15	17	21	23

For $k > 3$, let $m(k, q)$ denote the maximum length of an NMDS code of dimension k over $\mathbf{F}_q$. For some small values of q and n either the exact value of $m(k, q)$ or some strict bounds on $m(k, q)$ are known (see [20], [21] and the references therein).

	q								
k	2	3	4	5	7	8	9	11	13
2	6^1	8^1	10^1	12^1	16^1	18^1	20^1	24^1	28^1
3	7^1	9^1	9^3	11^2	15^1	$\mathbf{15}^{19}$	$\mathbf{17}^4$	$\mathbf{21}^2$	$\mathbf{23}^7$
4	8^1	10^1	10^2	12^1	$\mathbf{14}^3$	$\mathbf{16}^2$	$\mathbf{16}^{19}$	**20**	$21 - 24$
5		11^1	11^1	$\mathbf{11}^{60}$	$\mathbf{13}^{988}$	$\mathbf{15}^3$	$\mathbf{16}^1$	$18 - 21$	$21 - 25$
6		12^1	12^1	$\mathbf{12}^{31}$	**13**	**14**	**16**	$18 - 22$	$21 - 26$
7			9^3	$\mathbf{11}^6$	**14**	**15**	**17**	$18 - 23$	$21 - 27$
8			10^1	12^1	$\mathbf{13}^{988}$	**16**	**18**	$18 - 24$	$21 - 28$
9				11^2	$\mathbf{13}^{294}$	$\mathbf{14}^{58}$	**19**	$19 - 25$	$21 - 29$
10				12^1	$\mathbf{14}^3$	$\mathbf{15}^3$	**20**	$20 - 26$	$21 - 30$
11					$\mathbf{14}^4$	$\mathbf{15}^4$	$\mathbf{16}^1$	$18 - 27$	$21 - 31$
12					15^1	$\mathbf{16}^2$	$\mathbf{16}^{19}$	$18 - 28$	$21 - 32$
13					15	15	$\mathbf{16}^{382}$	$18 - 29$	$21 - 33$
14					16^1	16	$\mathbf{17}^4$	$18 - 30$	$21 - 34$
15						17	17	$18 - 31$	$21 - 35$
16						18^1	18	$20 - 32$	$21 - 36$

It should be noted the results obtained so far suggest that $m(k,q)$ is bigger than $N_q(1)$. That is, that unlike the MDS case, there exists NMDS codes which are longer than NMDS codes arising from algebraic curves.

References

[1] S. Ball, "On sets of points in finite planes ", Ph.D. Thesis, University of Sussex, UK, (1994)

[2] G.L. Feng and T.R.N. Rao, *Improved geometric Goppa codes*, Part I: Basic Theory, IEEE Trans. Inform. Theory **41**, 1678–1693 (1995).

[3] A. Garcia, S.J. Kim and R.F. Lax, *Consecutive Weierstrass gaps and minimum distance of Goppa codes*, J. Pure Appl. Algebra **84**, 199–207 (1993).

[4] A. Garcia and H. Stichtenoth, *On the asymptotic behaviour of some towers of functions fields over finite fields*, J. Number Theory **61**, 248–273 (1996).

[5] G. van der Geer, *Curves over Finite Fields and Codes*, Proc. 3ECM, Barcelona, (2000).

[6] G. van der Geer and M. van der Vlugt, How to construct curves over finite fields with many points, *Arithmetic Geometry* (Cortona 1994) (F. Catanese Ed.), 169–189, Cambridge Univ. Press, Cambridge, 1997.

[7] M. Giulietti, *On NMDS elliptic codes*, preprint.

[8] V.D. Goppa, *Algebraic-Geometric Codes*, Math. USRR-Izv. **21**(1), 75–93 (1983).

[9] V.D. Goppa, "Geometry and codes", Kluwer Academic Publishers, 1988.

[10] R. Hartshorne, "Algebraic Geometry", Grad. Texts in Math. Vol. 52, Springer-Verlag, New York/Berlin, 1977.

[11] J.W.P. Hirschfelf, "Projective Geometries over Finite Fields", second edition, Oxford University Press, Oxford (1998).

[12] J.W.P. Hirschfeld and L. Storme, *The packing problem in statistics, coding theory and finite projective spaces: update 2001*, in *Finite Geometries*, Kluwer, Dordrecht, (Chelwood Gate, 2000), 201–246 (2001)

[13] T. Høholdt, J.H. van Lint and R. Pellikaan, *Algebraic geometry codes*, in Handbook of Coding Theory (V.S. Pless, W.C. Huffman and R.A. Brualdi Eds.), vol. 1, 871–961, Elsevier, Amsterdam 1998.

[14] T. Høholdt and R. Pellikaan, *On the decoding of algebraic-geometric codes*, IEEE Trans. Inform. Theory **41**, 1589–1614 (1995).

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

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

[17] F.J. MacWilliams and N.J. Sloane, "The theory of error-correcting codes", North-Holland, Amsterdam, 1977.

[18] C. Moreno, "Algebraic curves over finite fields", Cambridge Tracts in Math., Vol. 97, Cambridge University Press, Cambridge, 1991.

[19] C. Munuera, *On the main conjecture on geometric MDS codes*, IEEE Trans. Inform. Theory **38**(5), 1573–1577 (1992).

[20] S. Marcugini, A. Milani and F. Pambianco, *Existence and classification of NMDS codes over $GF(5)$ and $GF(7)$*, Proc. VII ACCT, 232–239 (2000).

[21] S. Marcugini, A. Milani and F. Pambianco, *NMDS codes of maximal length over $GF(q)$, $8 \leq q \leq 11$*, IEEE Trans. Inform. Theory **48**(4), 963–966 (2002).

[22] R. Pellikaan and F. Torres, *On Weierstrass semigroups and the redundancy of improved geometric Goppa codes*, IEEE Trans. Inform. Theory **45**(7), 2512–2519 (1999).

[23] A. Seindenberg, "Elements of algebraic curves", Addison Wesley, Reading, MA, 1969.
[24] H. Stichtenoth, *A note on Hermitian codes over* $GF(q^2)$, IEEE Trans. Inform. Theory **34**(5), 1345–1348 (1988).
[25] H. Stichtenoth, "Algebraic function fields and codes", Universitext, Springer-Verlag, Berlin-Heidelberg, 1993.
[26] F. Torres, *Notes on Goppa Codes*, Quaderno del Seminario di Geometrie Combinatorie "G. Talllini" n. 136/marzo 2000, Dipartimento di Matematica Istituto "G. Castelnuovo", La Sapienza, Roma (2000)
[27] M.A. Tsfasman and S.G. Vladut, "Algebraic-geometric codes", Kluwer Academic Publishers, Dordrecht-Boston-London, 1991.
[28] M.A. Tsfasman, S.G. Vladut and T. Zink, *On Goppa codes which are better than the Varshamov-Gilbert bound*, Math. Nachr. **109**, 21–28 (1982).
[29] K. Yang and P.V. Kumar, On the true minimum distance of Hermitian codes, "Coding theory and algebraic geometry", Lecture Notes in Math. Vol. 1518, 99–107, Springer-Verlag, Berlin-Heidelberg, 1992.

Dipartimento di Matematica, Università degli Studi di Perugia, 06123 Perugia, Italy