Y. Achnine

On the main conjecture on algebraic-geometric MDS codes.

Master's thesis, 29 August 2011

Thesis advisor: Dr. R.S. de Jong.

Mathematisch Instituut, Universiteit Leiden

Contents

Introduction

Nowadays huge quantities of information have to be transmitted in each second. One can think of videos, music and text documents that must be sent through wire and wireless connections. Data must also reach very far targets like the hundreds of satellites around the earth and those in the far outer space. In coding theory tools have been developed to make it possible to compress information in order to transmit is efficiently. Compressing data means that information gets encoded (converted into another form) such that fewer bits are used than the original data would contain. After encoding, information has to be sent efficiently in the sense that this must happen not only quickly but also less expensively [1]. As soon as the information arrives at the receiver it gets decoded/decompressed to get the original information back. What usually happens is that errors occur in the decoding of information and this means that the decoded information does not match with what has been sent.

For example if you copy music from your computer to a CD, then a lot of bits ("0" 's and "1" 's) representing the music get encoded in the form of pits on one of the flat surfaces of the compact disk. Using laser technique the optic lens of the CD-player reads these pits and decodes them into bits again. If there is some dust or scratch on the CD, then this may result into weird noises. Luckily coding theory provides us with tools to recognize errors and sometimes, when possible, to locate and recover them. That is why you do not get weird noises if the CD has only small scratches or a bit of dust. The idea behind such tools is to encode information into a code (new information which includes control symbols) with good properties. These symbols serve to check whether errors occur and if possible the errors get located and repaired. A good code should have at least the following properties:

(1) Small probability of errors when decoding.
(2) Coding and decoding should not be complicated.
(3) Limited control symbols (redundancy).

In this thesis we deal with linear codes. These codes are widely used and mathematically well understood to a certain extent. We restrict[2] ourselves to algebraic-geometric codes (AG-codes) which are just linear codes arising from specific constructions in algebraic geometry. We will deal only with AG-codes that enjoy the property of being MDS codes. This property is defined for linear codes in general. It has been shown that MDS codes up to some equivalence are in fact equivalent to 'arcs'; these are objects in finite geometry which have been studied for decennia and which is still an active research area. We will make this equivalence more concrete and use results from both algebraic geometry and from finite geometry on AG-MDS codes. We will try to understand the main conjecture on MDS codes and we will deal with the case of AG-MDS codes from a geometric point of view. This will be done by comparing several attacks to solve this conjecture and by catching the

[1] A space scientist from the university of Leicester has worked out that sending texts via mobile phones is at least four times more expensive than receiving data from Hubble Space Telescope (compare £ 85 per MB to £ 374.49 per MB), See the online source http://www2.le.ac.uk/ebulletin/news/press-releases/2000-2009/2008/05/nparticle.2008-05-12.4476906328

[2] A result of

geometric ideas behind these attacks. Finally we will state and prove a result that is an improvement of a result on the main conjecture in a special case of AG-MDS codes.

Summary

In Chapter I we define linear codes and MDS codes. We will also state the main conjecture of MDS codes and give a historical overview on its origin and mention some of the results that are achieved by trying to solve it.
In Chapter II we recall important algebraic-geometric concepts and theorems which will serve us for the rest of the thesis. In Chapter III we make a connection between MDS codes and arcs (an object from finite geometry). We give some important results on arcs and use the connection we have established to conclude results on MDS codes. In Chapter IV we restrict our attention to AG-MDS codes. We define these codes and derive some of their important properties. Results on MDS codes from Chapter III will be rephrased and made explicit using algebraic-geometric notions developed in Chapter II. In Chapter V we deal in more detail with the main conjecture of MDS codes for AG-codes. Attacks on this conjecture will be studied and compared. We will see that they have more in common than what may appear at first sight. Finally we will derive a new theorem which has been developed during my research and we will also relate this theorem to the main conjecture. In Chapter VI we will work out concrete examples of AG-MDS codes. This will be done using the Magma software package.

Acknowledgements

I would like to thank my advisor Dr. Robin de Jong for his great encouragement and help. It was very useful and helpful to have regular meetings during the whole period of doing research for this thesis. I would like to thank him for his great patience, excellent explanation skills and frequent corrections of my thesis. I would like to thank the Prof. Dr. Ronald Cramer for reading the thesis and for his instructive questions. I also would like to thank Dr. R.M. van Luijk for his critical reading of my thesis and his several remarks. They have been very useful for both my thesis as for my graduation talk.

1. Linear codes and MDS codes

A good reference to most of the theory on linear codes in this section is [39, Chapter 3].

1.1. **Linear codes.**

Let $\mathbb{F}_q$ be a finite field, $q = p^m$ and p is prime. For an element $z = (z_1, ..., z_n)$ of the $\mathbb{F}_q$-vector space $\mathbb{F}_q^n$ we define its *Hamming weight* $w(z)$ by

$$w(z) := \#\{i | i \in \{1, 2, ..., n\} : z_i \neq 0\}.$$

This leads to the notion of a distance in $\mathbb{F}_q^n$: for $x, y \in \mathbb{F}_q^n$ we define

$$d(x, y) := w(x - y).$$

Note that $d(x + z, y + z) = d(x, y)$ makes the distance function d translation invariant.

Definition 1.1. A *linear code* C of length n over $\mathbb{F}_q$ is a nonzero linear subspace in $\mathbb{F}_q^n$. An element of C is called a code word. The dimension of C is by definition $k = \dim(C) = \dim_{\mathbb{F}_q}(C)$. The *minimal distance* $d = d(C)$ of C is defined by:

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

Note that $d(C)$ is the same as $\min\{w(x) : x \in C, x \neq 0\}$.
We usually say that C is a $[n, k, d]$-linear code. The minimal distance determines in fact the maximal number of errors that can be corrected independently of the position of the errors. If we are not interested in d we just write $[n, k]$ instead of $[n, k, d]$. In this thesis a 'code' is always a 'linear code'.

Let $\mathcal{A}$ be the subgroup in the group of linear automorphisms of $\mathbb{F}_q^n$ generated by permutations of coordinates and multiplications of coordinates by nonzero elements of $\mathbb{F}_q$. Then $\mathcal{A}$ acts on linear subspaces of $\mathbb{F}_q^n$ and hence on codes. Two $[n, k]$-codes C and C' over $\mathbb{F}_q$ are called equivalent if $\alpha(C) = C'$ for some $\alpha \in \mathcal{A}$. That is, $C = C' \cdot P \cdot D$ with P a permutation matrix with entries in $\mathbb{F}_q$ and D a nonsingular diagonal matrix with entries in $\mathbb{F}_q$.

A matrix G of which the rows generate a $[n, k]$-code C is called a *generator matrix* for C. This matrix G is not unique but under the set of generator matrices of C there exists a unique generator matrix in the reduced row echelon form.

Linear codes are a kind of codes which enjoy the property of being *systematic*. We can explain this property as follows: Let $G = (I_k|A)$ be a $k \times n$ generator matrix in reduced echelon form of a linear code C. We get a linear map

$$\mathbb{F}_q^k \to \mathbb{F}_q^n, \quad u \to uG.$$

An element $u = (u_1, ..., u_k) \in \mathbb{F}_q^k$ has as image an $1 \times n$-vector $(u_1, u_2, ..., u_k, *, ..., *) = (u, uA)$, where " $*$ " are some elements of $\mathbb{F}_q$. The part uA consists of the $n - k$ control symbols. The code C has the property that the information word u is a part of the code word uG. This property makes the code systematic.

Let C be an embedding for a code C. We can interpret C as the kernel of the quotient map $\mathbb{F}_q^n \to \mathbb{F}_q^n/C$. A *parity-check* for a linear code C is a linear equation

$$a_1x_1 + ... + a_nx_n = 0 \, (a_i \in \mathbb{F}_q).$$

that holds for all $(x_1, ..., x_n) \in C$.

Since a linear code C is just a (finite) $\mathbb{F}_q$-vector subspace of $\mathbb{F}_q^n$ we can speak of the *dual code* $C^\perp$ of C:

$$C^\perp := \{a \in \mathbb{F}_q^n : (a, x) = 0 \text{ for all } x \in C\}.$$

where (a, x) is the dot-product $\sum_{i=1}^n a_i x_i$ in $\mathbb{F}_q^n$. Note that $C^\perp$ is an $(n, n-k)$-linear code over $\mathbb{F}_q$. A generator matrix H for $C^\perp$ is called *the parity-check matrix* of C. As $C = (C^\perp)^\perp$,we can easily deduce that

$$C = \{\mathbb{F}_q^n : Hx^T = 0\}.$$

Notice that if C is an $[n, k]$-code with generator matrix G, then an $[n-k, n]$-matrix with rank $n-k$ is a parity-check matrix H for C if and only if $HG^T = 0_{n-k\times k}$.

Remark 1.2.
A useful observation tells us that if an $[n, k]$-code C has minimal distance d, then for its parity-check matrix H it holds that d is the minimal number of any linearly dependent set of columns of H. To show this fact let k_i for $i = 1, ..., n$ be the columns of H. Then we have $x = (x_1, ..., x_n) \in C$ if and only if $Hx^T = \sum_{i=1}^n x_i k_i = 0 \in \mathbb{F}_q^n$. An element $x \in C$ which has positive weight yields a nontrivial relation between the columns of H.

1.2. **MDS codes.**

Now we define MDS codes and state some general facts on them. Facts on the history of MDS codes can be found in [19, Chapter 11, p.329]. The name "maximum distance separable code" comes from the fact that an MDS code has the maximum possible distance between code words for fixed n and k, and from the fact that code words can be separated into information word and control symbols. Investigating how large the length of MDS codes with a given dimension over a fixed $\mathbb{F}_q$ can get;can be closely associated to several combinatorial problems. An example of such problem is the following:

Problem 1.3. *Consider the vector space $\mathbb{F}_q^n$. What is the largest number of vectors in this space with the property that any n of them form a basis for the space?*

Soon we will give a partial answer to this problem.

Proposition 1.4. *For a $[n, k, d]$-linear code C we have*

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

Proof. Let H be a parity-check matrix for C. Then H has rank $n-k$ which is the maximal number of linearly independent columns of H. By the observation (Remark 1.2) in the previous subsection we have $d \leq n - k + 1$ and hence $k \leq n - d + 1$. □

Definition 1.5. The bound $d \leq n - k + 1$ is called the *Singleton bound*.

Definition 1.6. An $[n, k, d]$-linear code which satisfies the Singleton bound (i.e $d = n - k + 1$) is called a maximum distance separable code (MDS).

Over any field there exist $[n, 1, n]$, $[n, n-1, 2]$ and $[n, n, 1]$ MDS codes. These are called *trivial* MDS codes. Nontrivial codes have $2 \leq k \leq n-2$. The mathematician Richard Collom Singleton is apparently the first one who explicitly studied MDS codes [30]. The bound in Definition 1.5 is named after him. However in 1952 Bush [5] had already discovered the so called Reed-Solomon codes (which are MDS codes) and he also had given an extension of them using the 'language' of orthogonal arrays.

Proposition 1.7. *If G is an $k \times n$ generator matrix of an $[n, k, d = n-k+1]$-MDS code C, then we have:*

(1) *Each k-tuple of column vectors is linearly independent.*
(2) *The dual code $C^{\perp}$ is MDS, that is $d(C^{\perp}) = k + 1$.*

Proof.

(1) To see this remember that the minimum distance is $d = n - k + 1$. So any nonzero linear combination of the rows of G has at most $k - 1$ zeros. We know that the row-rank of a matrix is equal to the column-rank. So for the columns of G this means that any k columns are linearly independent.
(2) (See [20, Lemma 6.7, p. 245]) Let H be an $(n-k) \times n$ parity check matrix for C. Then H is a generator matrix for $C^{\perp}$. If for some $m \in \mathbb{F}_q^{n-k}$ we have $c = mH \in C^{\perp}$ with $w(c) \leq k$, then c has zero elements in $\geq n - k$ positions. Let the zero elements of c have indices $\{i_1, ..., i_{n-k}\}$. Write

$$H = [h_1 \ h_2 \ ... \ h_n].$$

The zero elements of c are obtained from

$$0 = m[h_{i_1} \ h_{i_2} \ ...h_{i_{n-1}}] = m\tilde{H}$$

with $\tilde{H}$ a singular $(n-k) \times (n-k)$ submatrix of H. Using again that the row-rank of a matrix is equal to the column-rank there must be $n - k < n - k + 1 = d$ columns of H which are linearly dependent. According to Remark 1.2 this contradicts the assumption that C has minimum distance $n - k + 1$ so $d(C^{\perp}) > k$. But then we must have $d(C^{\perp}) = k + 1$.

□

Corollary 1.8. *Let C be an $[n, k]$-MDS code. Then every $n-k$ columns of a parity check matrix of C are linearly independent.*

A useful tool of studying the properties of a linear code C over $\mathbb{F}_q$ is the distribution of the weights of elements in C. *The weight distribution* of a linear code C is the sequence of numbers

$$A_t := \#\{c \in C | w(c) = t\}.$$

The (single variable) weight distribution enumerator is defined as

$$A(z) = \sum_{x \in C} z^{w(x)} = A_0 + A_1 z + ... + A_n z^n (\in \mathbb{Z}[z]).$$

MacWilliams proved that for the weight distribution enumerator $B(z)$ of the dual code $C^{\perp}$ the identity

$$B(z) = (1 + (q-1)z)^n A\left(\frac{1-z}{1+(q-1)z}\right)$$

holds. More specifically, if we define $B_t := \#\{c \in C^{\perp} | w(c) = t\}$, then for all $v \in \{0, ..., n\}$ we get the *MacWilliams equations*:

$$\sum_{i=0}^{n-v} \binom{n-i}{v} A_i = q^{k-v} \sum_{i=0}^{v} \binom{n-i}{n-v} B_i.$$

For a proof of this result see [15, Chapter 7, Theorem 1.3, p. 254]. An MDS code has the property that its weight distribution is completely determined by k and n. If C is MDS, then $A_i = 0$ for $i = 1, ..., n-k$ and $B_i = 0$ for $i = 1, ..., k$. Using the previous identity one can prove (after rearrangement of terms) that :

Theorem 1.9. *Let C be an $[n, k, d = n-k+1]$ MDS code over $\mathbb{F}_q$. Then for the number of words of weight w in C we have:*

$$A_w = \binom{n}{w}(q-1)\sum_{j=0}^{w-d}(-1)^j \binom{w-1}{j} q^{w-d-j}.$$

Corollary 1.10. *Let C be an $[n, k, d = n-k+1]$ MDS code over $\mathbb{F}_q$*

(1) *If $k \geq 2$, then $n \leq q + k - 1$.*
(2) *If $k \leq n-2$, then $k+1 \leq q$.*

Proof. For the first statement substitute in Theorem 1.9 $w = n-k+2$ so you get $A_{n-k+2} = \binom{n}{k-2}(q-1)(q-n+k-1)$ and note that A_{n-k+2} must be nonnegative. The second statement follows from examining the weight distribution of $C^{\perp}$. □

An improvement of this result can be found in [19, Theorem 11, p. 326]:

Proposition 1.11. *If C is a nontrivial $[n, k \geq 3, n-k+1]$ MDS code over $\mathbb{F}_q$ with q odd, then $n \leq q + k - 2$.*

Now we see why $[n, 1, n]$ (and its dual $[n, n-1, 2]$) and $[n, n, 1]$ codes are called trivial MDS codes. In Theorem 1.9 if $k = 1$, then there are arbitrarily long MDS codes, namely the *repetition* codes[3]. Note that the zero code and the whole space $\mathbb{F}_q^n$ ($[n, n, 1]$) are also MDS and can get arbritarily long. If $k \leq n-2$, then $k \leq q-1$. So nontrivial $[n, k]-$ MDS codes exist only if $2 \leq k \leq \min(n-2, q-1)$. As $n \leq q+k-1$ we find $k \leq \min(n-2, q-1) \leq q-1$ and $n \leq 2q-2$. This gives a primary answer to Problem 1.3: the length of nontrivial MDS codes is bounded when q is fixed.

We already see for $k = 3$ that $n \leq q+2$. In the following subsection we will see that one conjectures that for $1 < k < q$ (hence for nontrivial MDS codes) the bound $n \leq q+k-1$ can be sharpened to $n \leq q+1$ or $n \leq q+2$ depending on the parity of q.

[3]For example: A binary repetition code of length n consists of just two words $(0, 0, ..., 0)$ and $(1, 1, ..., 1)$ of length n.

1.3. **The main conjecture of MDS codes.**
It is easy to construct codes which do not satisfy the Singleton bound. It is also not that hard to construct codes which do satisfy this bound. For an $[n, k]$-MDS code the following conjecture is still not completely solved:

Conjecture 1.12. *For every linear $[n, k]$-MDS code over $\mathbb{F}_q$ if $1 < k < q$, then $n \leq q + 1$, except when q is even and $k = 3$ or $k = q - 1$ in which cases $n \leq q + 2$.*

This conjecture is called the main conjecture of MDS codes. It has been partially solved due to the work of several mathematicians. At the moment of writing this thesis a result of Simeon Ball [3] implies that the main conjecture of MDS codes holds for all primes q. The methods used in his (to appear) article are beyond the scope of this thesis since we are interested in algebraic-geometric approaches. We study a few simple cases by considering a generator matrix for an $[n, k]$-MDS code and viewing the columns of this matrix as a set S of n points in $\mathbb{P}^{k-1}$. The statement 'All k-tuple of column vectors is linearly independent' in Proposition 1.7 is then equivalent to the statement 'All k-tuples of the corresponding points in $\mathbb{P}^{k-1}$ are not contained in a hyperplane'.
Case $k = 2$:
Since $\#\mathbb{P}^1(\mathbb{F}_q) = q + 1$ we must have $n \leq q + 1$ and the conjecture holds for $k = 2$.

Case $k = 3$ and q is odd:
Observe that for any point in $\mathbb{P}^2(\mathbb{F}_q)$ there are exactly $q + 1$ lines passing through this point. Suppose that $\#S = q + 2$ and there are no three distinct points in S which are collinear. For any $Q \in S$ a line passing through Q must pass exactly one other point in $S\backslash\{Q\}$ since there are no three points which are collinear and $\#(S\backslash\{Q\}) = q + 1$. Now we conclude that the points of S are coupled into pairs by lines. Hence $q + 2$ is even and so is q. We see in particular that $n \leq q + 1$.

Case $k = 3$ and q is even:
We show that $n \leq q+2$. This is a straightforward application of Corollary 1.10 but we proceed giving another proof. Suppose that $\#S = q+3$ and that S is in general position. Take a $Q \in S$ and connect Q with each of the other points through a line. Since S is in general position each of these $q + 2$ lines intersects S in exactly two points, one of which is Q. So by removing Q we get a set $\mathcal{L}$ of $q+2$ 'lines' each of them is missing one point. In $\mathbb{P}^2(\mathbb{F}_q)$ we know that each line contains $q+1$ points and that $\#\mathbb{P}^2(\mathbb{F}_q) = q^2+q+1$. But we have $(q+1-1)(q+2) = q^2+2q > q^2+q+1 = \#\mathbb{P}^2(\mathbb{F}_q)$ so S can not contain $q + 3$ points.

The cases $k = 4$ and $k = 5$ have been also solved using other techniques from finite geometry. We saw that conjecture deals only with nontrivial codes and since the dual of an MDS code is also MDS one may assume that $5 < k \leq n/2$. In the literature ([13] and [7]) there are proofs for $q \leq 27$ hence $q > 27$ may also be assumed.

2. Linear codes and algebraic geometry

2.1. **Divisors and rational maps.**

In this section we shall introduce terminology from algebraic geometry and coding theory. We shall define a linear code using algebraic geometry. We refer to [11, II.6] and [11, IV] for more details and results. Other useful sources for this chapter which will be frequently referred to are [38, 2] and [2, I]. Some definitions are slightly different from the ones used by Hartshorne. We shall write K for a field and $\overline{K}$ for a fixed algebraic closure of K.

We introduce the notion of a projective space over a field using [29, I.2].

Definition 2.1. *Affine n-space* (over K) is the set of n-tuples

$$\mathbb{A}^n = \mathbb{A}^n(\overline{K}) = \{(x_1, ..., x_n) : x_i \in \overline{K}\}.$$

Definition 2.2. *Projective n-space* (over K), denoted by $\mathbb{P}^n$ or $\mathbb{P}^n(\overline{K})$, is the set of all $(n+1)$-tuples

$$(x_0, ..., x_n) \in \mathbb{A}^{n+1}$$

such that at least one x_i is nonzero, modulo the equivalence relation:

$$(x_0, ..., x_n) \sim (y_0, ..., y_n)$$

if there exists a $\lambda \in \overline{K}^*$ such that for all i we have $x_i = \lambda y_i$. We denote by $(x_0 : x_1 : ... : x_n)$ an equivalence class

$$\{(\lambda x_0, ..., \lambda x_n) : \lambda \in \overline{K}^*\}.$$

The individuals $x_0, ..., x_n$ are called homogenous coordinates for the corresponding point in $\mathbb{P}^n$.

The set of *K-rational points* in $\mathbb{P}^n$ is the set

$$\mathbb{P}^n(K) := \{(x_0 : ... : x_n) \in \mathbb{P}^n(K) : \text{ all } x_i \in K\}.$$

Definition 2.3. Let $P = (x_0 : ... : x_n) \in \mathbb{P}^n(\overline{K})$. The *minimal field of definition* for P (over K) is the field

$$K(P) := K(x_0/x_i, ..., x_n/x_i) \text{ for any } i \text{ with } x_i \neq 0.$$

Suppose that K is perfect. Then the Galois group of $\overline{K}/K$ (notation $G_{\overline{K}/K}$) acts on $\mathbb{P}^n(\overline{K})$ by acting on its homogeneous coordinates: $P^\sigma = (x_0 : ... : x_n)^\sigma = (x_0^\sigma : ... : x_n^\sigma)$ for any $\sigma \in G_{\overline{K}/K}$. One can check that

$$\mathbb{P}^n(K) = \{P \in \mathbb{P}^n(\overline{K}) : P^\sigma = P \text{ for all } \sigma \in G_{\overline{K}/K}\}$$

and that

$$K(P) = \text{ fixed field of } \{\sigma \in G_{\overline{K}/K} : P^\sigma = P\}.$$

Definition 2.4. By a *curve* over K we mean a projective nonsingular geometrically irreducible [4] one-dimensional variety over K.

[4] A curve X over a field K is called geometrically irreducible if for any field extension K' of K the curve $X \otimes K'$ obtained from X by base change remains irreducible.

For abbreviation we usually say 'X is a curve' without specifying the field K. But we keep in mind that we are working over K.

Definition 2.5. A (Weil) *divisor* on a curve X is a finite formal sum $D = \sum_{P \in X(\overline{K})} n_P P$, with $n_p \in \mathbb{Z}$ and $n_P = 0$ for all but a finite number of $\overline{K}-$valued points $P \in X(\overline{K})$.

We denote by $\mathrm{supp}(D)$ the *support* of a divisor D, that is the set of points with nonzero coefficients in $\mathbb{Z}$. The set of divisors on X is denoted by $\mathrm{Div}(X)$. This is an (additively written) abelian group with the obvious neutral element and addition. A divisor $D = \sum_{P \in X(\overline{K})} n_P P$ on X is called *effective* if $n_P \geq 0$ for all $P \in X$. The *degree* of such a divisor D (notation $\deg(D)$) is by definition the integer $\sum_{P \in X(\overline{K})} n_P$.

The Galois group of $\overline{K}/K$ acts in an obvious way on a divisor $D = \sum_{P \in X(\overline{K})} n_P P$ on X:

$$D^\sigma = \sum_{P \in X(\overline{K})} n_P P^\sigma.$$

Definition 2.6. A divisor D is called defined over K if $D^\sigma = D$ for all $\sigma \in G_{\overline{K}/K}$. The set of all divisors D on X defined over K is usually denoted by $\mathrm{Div}_K(X)$. By $\mathrm{Div}^d(X)$ we denote the subgroup of $\mathrm{Div}(X)$ of elements of degree d.

Let X is a curve over K. A function $f : X \to K$ is called regular at a point $P \in X$ if there is a neighborhood U with $P \in U \subset X$, and homogeneous polynomials $g, h \in S = K[x_0, ..., x_n]$, such that h is nowhere zero on U and $f = g/h$ on U. We say that f is regular on X if it is regular at every point. We denote by $\mathcal{O}_{P,X}$ the *local ring* in P. So $\mathcal{O}_{P,X}$ is the ring of germs of regular functions on X near P. Since X is smooth; $\mathcal{O}_{P,X}$ is a discrete valuation ring and it has a unique maximal ideal m_P. It is known that m_P is principal and we call a generator of m_P a *uniformizer* for X.The function field of X (notation $K(X)$) is the field of rational functions over X. A function $f \in K(X)$ is regular (defined) at P if it lies in $\mathcal{O}_{P,X}$. Let $f \in K(X)^*$ be any nonzero rational function on X. Then the quotient field of the local ring $\mathcal{O}_{P,X}$ coincides with $K(X)$. On $\mathcal{O}_{P,X}$ there is a function ord_P which is defined for $f \in \mathcal{O}^*_{P,X}$ by $\mathrm{ord}_P(f) = \max\{l | f \in m_P^l, l \in \mathbb{Z}_{\geq 1}\}$. If $f \in K(X)^*$, write $f = \frac{g}{h}$ with $g, h \in \mathcal{O}_p$ and define $\mathrm{ord}_P(f) = \mathrm{ord}_P(g) - \mathrm{ord}_P(h)$. This gives a discrete valuation $K(X)^* \to \mathbb{Z}$. Note that if t is a uniformizer for X, then $\mathrm{ord}_P(t) = 1$.

It is known that for $f \in K(X)^*$ a nonzero rational function on X that $\mathrm{ord}_P(f) \neq 0$ holds only for finitely many points $P \in X$. We define the divisor of a nonzero rational function f which will be denoted by (f) or $\mathrm{div}(f)$ by

$$(f) = \sum_{P \in X(\overline{K})} \mathrm{ord}_P(f) \cdot P.$$

Definition 2.7. A divisor D is called a *principal* divisor if $D = (f)$ for some $f \in K(X)^*$.

One can prove that principal divisors over a curve X have degree 0. This leads us to the following definition:

Definition 2.8. Two divisors D and D' over K on X are said to be *linearly equivalent*, written $D \sim D'$ if $D - D'$ is a principal divisor, i.e, if $D - D' = (f)$ where $f \in K(X)^*$ is a nonzero principal divisor. The equivalence class of a divisor D is denoted by $[D]$. The group $\mathrm{Div}(X)$ of all divisors divided by the subgroup of principal divisors is called the *divisor class group* of X (or the Picard group of X, notation $\mathrm{Pic}(X)$). We also write $\mathrm{Pic}^d(X)$ for $\mathrm{Div}^d(X)/\sim$.

Remark 2.9.
For a not necessarily smooth variety X, what we have defined is not the Picard group, but the Weil divisor class group. The Picard group in general is the group of isomorphism classes of line bundles on X. Studying the differences is beyond the scope of this thesis. We refer the reader to [11, II.6] or [4, II, Remark 1].

Later in this thesis we will use the notion of the Jacobian of a curve. This is a special variety which is closely connected to the Picard group. Some of its properties will be used in different proofs.

For the following we write $\mathrm{Specm}(K)$ for the set of the maximal ideals of K and we will mean by an algebraic variety G an algebraic reduced variety of finite type of dimension over a field K.

Definition 2.10. A group variety G over K is an algebraic variety together with regular maps

$$m : G \times_K G \to G$$
$$inv : G \to G$$

and an element $e \in G(K)$ such that the structure on $G(\overline{K})$ defined by m and inv is a group with identity e.

Such a quadruple (V, m, inv, e) is a group in the category of varieties over $\overline{K}$. This means that:

(1)
$$G \xrightarrow{(\mathrm{id},e)} G \times_k G \xrightarrow{m} G, \;\; G \xrightarrow{(e,\mathrm{id})} G \times_k G \xrightarrow{m} G$$
are both the identity map which makes e the identity element.

(2)
$$G \xrightarrow{\Delta} G \times_k G \underset{\mathrm{inv}\times\mathrm{id}}{\overset{\mathrm{id}\times\mathrm{inv}}{\rightrightarrows}} G \times_k G \xrightarrow{m} G$$
are equal to the composite
$$G \longrightarrow \mathrm{Specm}(K) \xrightarrow{e} G$$
which implies that inv is the map taking an element to its inverse.

(3) The diagram
$$\begin{array}{ccc} G \times_K G \times_K G & \xrightarrow{1\times m} & G \times_K G \\ \downarrow{\scriptstyle m\times 1} & & \downarrow{\scriptstyle m} \\ G \times_K G & \xrightarrow{m} & G \end{array}$$
commutes (the associativity).

An example of a group variety is the set of nondegenerate $n \times n$ matrices over $\overline{K}$ under the standard matrix multiplication law.

Definition 2.11. A connected algebraic group G which is also a projective variety is called an *abelian variety*.

The name abelian variety is justified by the (nontrivial) fact that it is abelian as a group.

Theorem 2.12. *For each curve there exists a unique abelian variety $J_X(K)$ such that*

(1) *$J_X(K)$ is isomorphic to $Pic^0(X)$ as a group;*
(2) *The map*
$$i_{P_0} : X \to J_X(K)$$
$$P \mapsto [P - P_0],$$
where P_0 is an arbitrary fixed point of X, is regular;
(3) *For any regular map $\phi : X \to A$ from X to an abelian variety A such that $\phi(P_0)$ is the neutral element of A, there is a morphism of abelian varieties $\lambda : J_X(K) \to A$ with $\phi = \lambda \circ i_{P_0}$.*

The abelian variety $J_X(K)$ is called the Jacobian *of X.*

We are most interested in the number of rational points on $J_X(K)$ when X (and hence $J_X(K)$) is defined over $K = \mathbb{F}_q$.

Theorem 2.13. *For the number of $\mathbb{F}_q$-points of the Jacobian $J_X(\mathbb{F}_q)$ corresponding to a curve X over $\mathbb{F}_q$ of genus g we have:*
$$(\sqrt{q} - 1)^{2g} \leq h \leq (\sqrt{q} + 1)^{2g}.$$

Proof. See [38, III.1, Proposition 23]. □

Definition 2.14. Let D be any divisor on a curve X over K. Define
$$L(D) = \{f \in K(X)^* : (f) + D \geq 0\} \cup \{0\}.$$

This is a K-vector space of rational functions of which the pole divisor (the part of the associated rational divisor where points have negative coefficients) is bounded by D. We call it *the space associated to the divisor D*. We denote by $l(D)$ or $\dim L(D)$ its dimension. It is known that $l(D)$ depends only on the equivalence class of D and that this dimension is finite for any $D \in \mathrm{Div}(X)$. Furthermore, if $\deg(D) < 0$ then $L(D) = \{0\}$ and $l(D) = 0$. In the rest of this thesis we will use divisors defined on $\mathbb{F}_q$ (see 2.6) instead of working over an algebraically closed field $\overline{\mathbb{F}}_q$. The next lemma helps us to get a suitable definition of $L(D)$ when K is not necessary algebraically closed.

Lemma 2.15. *Let X be a curve over a perfect field K. Let $D \in Div_K(X)$. Then $L(D)$ has a basis consisting of functions in $K(X)$.*

Proof. See [29, I.5, Proposition 5.8 and Lemma 5.8.1] □

Definition 2.16. Note also that if a curve is defined over a field K and two equivalent divisors $D \sim D'$ on X are also defined over K, then there exist an $f \in K(X)^*$ such that $D - D' = (f)$.

Let D be a divisor on a curve X. Let $V \subset L(D)$ be a subspace. The set of effective divisors of the form $(f) + D$ with $f \in V \setminus \{0\}$ is called a *linear system* and is denoted by $|V|$. If $V = L(D)$, then $|V|$ is called a *complete linear system* and it is denoted by $|D|$.

One can verify that $|V| \cong \mathbb{P}(V)$ (the projectivization of V) by noticing that for $f, g \in K(X)^*$ we have $(f) = (g)$ if and only if there is a constant $\lambda \in K^*$ such that $f = \lambda g$. For $V \neq 0$ this gives an isomorphism from $\mathbb{P}(V)$ onto $|V|$ by sending nonzero $f \in V$ to the divisor $(f) + D$. It follows that $\dim |V| = \dim V - 1$.

Explicitly we have for $L(D)$:

$$\begin{aligned} \mathbb{P}(L(D))^* &= \{ \text{ The dual space of } \mathbb{P}(L(D))\} \\ &= \{ \text{ Hyperplanes in } \mathbb{P}(L(D))\} \\ &= \mathbb{P}(L(D)^*) \\ &= \mathbb{P}(\{ \text{ Linear forms on } L(D)\}) \\ &= \mathbb{P}(\{ \text{ Hom}_K(L(D), K)\}). \end{aligned}$$

Definition 2.17. Let D be a divisor on a curve X. Let $0 \neq V \subset L(D)$ be a nonzero subspace. Let $|V|$ be the corresponding linear system. A point $P \in X$ is called a *base point* of $|V|$ if $P \in \text{supp}(E)$ for all $E \in |V|$. If $|V|$ has no base point, then $|V|$ is called base point free.

Lemma 2.18. *Let D be a divisor on a curve X. The complete linear system $|D|$ has no base point if and only if for every point $P \in X$ we have:*

$$\dim |D - P| = \dim |D| - 1.$$

Proof. See [11, IV.3, 3.1]. □

If D be a divisor of degree d and $|V|$ is a linear system where V is a vector subspace of $L(D)$ and $\dim(V) = r + 1$, then write g^r_d for $|V|$. We call a g^1_d a pencil.

2.1.1. *From linear systems to morphisms.*

We conclude this subsection by giving an explicit connection between linear systems on a curve X and rational maps from X to projective spaces. This will be very useful when treating the main conjecture of MDS codes as a conjecture in terms of algebraic geometry.

Let $\phi : X \dashrightarrow \mathbb{P}^n$ be a rational map given by

$$\phi : X \dashrightarrow (f_0(P) : ... : f_n(P)). \tag{1}$$

Assume that $\text{Im}(\phi)$ is not degenerate (i.e, not contained in a hyperplane, otherwise we can consider ϕ as a rational map from X to $\mathbb{P}^m$ with $m < n$). Let

$$(f_i) = \sum a_{P,i} P, \quad i = 0, ..., n$$

and let

$$D = -\sum a_P P$$

where $a_P = \min_{0 \leq i \leq n} a_{P,i}$. By construction it follows that $(f_i) + D \geq 0$, hence $f_i \in L(D)$. It also follows that D is in fact base point free. Let $V_\phi = \text{span}(f_0, ..., f_n) \subset L(D)$. Then to ϕ we assign the linear system $|V_\phi| \subset |L(D)|$.

On the other hand let $|V| \subset |D|$ and let $n = \dim |V|$. Let $(f_0, ..., f_n)$ be a basis in V. Suppose that $|V|$ is base point free. Then

$$P \to (f_0(P) : ... : f_n(P)).$$

defines a rational map $\phi : X \dashrightarrow \mathbb{P}^n$. This is well defined since demanding that $|V|$ has no base points guarantees that a $P \in X$ is never a zero for all $f_i(P)$, $i = 0, ..., n$. The map ϕ above 'is' even a morphism. This follows directly from the next theorem:

Theorem 2.19. *Any rational map from a curve to a projective space extends to a morphism.*

Proof. See [38, 2.1.60]. □

We conclude that we have the following $1-1$ correspondence:

$$\{ \text{ Base point free linear systems of dimension. } n \text{ on } X\} / \sim$$
$$\updownarrow$$
$$\{ \text{ Morphisms } \phi : X \to \mathbb{P}^n \text{ with nondegenerate image, up to linear coordinate changes. } \}$$

It may be useful to bear in mind that the $(f_i) + D$ can be viewed as inverse images of hyperplanes, for if $\lambda = (\lambda_0 : ... : \lambda_n) \in \mathbb{P}^n(K)$ and H_λ is a hyperplane given by $\sum \lambda_i x_i = 0$, then $f^*(H_\lambda) = (\sum \lambda_i f_i) + D$. In the case that $n = 1$ we get $\deg(f) = \deg(D)$.

Proposition 2.20. *Let $\phi : X \to \mathbb{P}^n$ be the morphism [5] corresponding to the base-point-free linear system $L = \mathbb{P}(V) \subset \mathbb{P}(L(D))$. Then ϕ is an embedding if and only if:*

1. *For any distinct points $P, Q \in X$ there is a $D' \in L$ with $D' \geq P$ and not $D' \geq Q$. (L separates points).*
2. *For any $P \in X$ there is a $D' \in L$ with $D' \geq P$ but $D \geq 2P$. (L separates tangent vectors).*

Proof. See [16, 4, Proposition 3.5] □

Definition 2.21. A divisor D on a curve X is called *very ample* if there exists a projective embedding

$$f : X \to \mathbb{P}^m$$

such that D is linearly equivalent to $f^*(H)$ for some hyperplane H of $\mathbb{P}^m$.

In particular if D is a very ample divisor of degree d and dimension $k = l(D)$ on a curve X, then D gives rise to embedding $f_D : X \hookrightarrow \mathbb{P}^{k-1}$ such that the image of X is a curve in $\mathbb{P}^{k-1}$ of degree d. Later on in this section we give a way of verifying whether a divisor is very ample which works in many important cases.

2.2. **Differential forms and Riemann-Roch.** The Riemann-Roch theorem is indispensable when studying algebraic geometric codes. Before we state it we need some definitions and lemmas. These can be found in [29, I.4].

Definition 2.22. Let X be a curve. The space of differential forms on X, denoted by Ω_X, is the $\overline{K}(X)$-vector space generated by symbols of the form dx for $x \in \overline{K}(X)$, subject to the usual relations:

(1) $d(x + y) = dx + dy$ for all $x, y \in \overline{K}(X)$.

[5] it is unique up to an automorphism of $\mathbb{P}^n$.

(2) $d(xy) = xdy + ydx$ for all $x, y \in \overline{K}(X)$.
(3) $da = 0$ for all $a \in \overline{K}$.

We state a few results on Ω_X:

Proposition 2.23. *Let $P \in X$, and let $t \in \overline{K}(X)$ be a uniformizer at P.*

(1) *The $\overline{K}(X)$-vector space Ω_X is one dimensional. If $x \in \overline{K}(X)$, then dx is a $\overline{K}(X)$ basis for Ω_X if and only if $\overline{K}(X)/\overline{K}(x)$ is a finite separable extension.*
(2) *For every $\omega \in \Omega_X$ there exists a unique function $g \in \overline{K}(X)$, depending on ω and t, such that*
$$\omega = gdt.$$
(Another notation for g is $\frac{\omega}{dt}$).
(3) *Let $f \in \overline{K}(X)$ be regular at P then $\frac{df}{dt}$ is also regular at P.*
(4) *The quantity*
$$ord_P(\frac{\omega}{dt})$$
depends only on ω and P. It is independent of the choice of the uniformizer t. We call $ord_P(\frac{\omega}{dt})$ the order of ω at P and we write for abbreviation $ord_P(\omega)$.
(5) *Assume that $\omega \neq 0$. For all but finitely many $P \in X$ we have:*
$$ord_P(\omega) = 0.$$

Proof. See [29, I.4, Proposition 4.2] and [29, I.4, Proposition 4.3]. □

The next proposition tells us how to calculate the order of a differential form on X:

Lemma 2.24. *Let $x, f \in \overline{K}(X)$ with $x(P) = 0$ and let $p = char(K)$. Then*

(1) *$ord_P(fdx) = ord_P(f) + ord_P(x) - 1$, if $p = 0$ or $p \nmid ord_P(x)$.*
(2) *$ord_P(fdx) \geq ord_P(f) + ord_P(x)$, if $p > 0$ and $p | ord_P(X)$.*

Proof. See [29, I.4, Proposition 4.3]. □

Definition 2.25. Let $\omega \in \Omega_X$ and $P \in X$. We define the residue of ω at P (notation $\text{res}_P(\omega)$) as follows: Write $\omega = gdt$ with t a local parameter at P and $g \in \overline{K}(X)$. If $v_P(g) \geq 0$, then $\text{res}_P(\omega) := 0$. Otherwise, if $v_P(g) = -n \leq -1$, write $g = a_{-n}t^{-n} + ... + a_{-1}t^{-1} + h$ with $h \in K(X)$ regular at P, then define $\text{res}_P(\omega) := a_{-1}$. This definition does not depend on t (See [11, III, 7.14]).

The next useful theorem is called the Residue Theorem.

Proposition 2.26. *For any $\omega \in \Omega_X$ we have $\sum_{P \in X(\overline{K})} res_P(\omega) = 0$.*

Proof. See [11, III, Theorem 7.14.2]. □

Definition 2.27. Let $0 \neq \omega \in \Omega_X$. The divisor associated to ω is
$$\text{div}_P(\omega) = \sum_{P \in X(\overline{K})} \text{ord}_P(\omega)P \in \text{Div}_{\overline{K}(X)}.$$

Differentials $\omega \in \Omega_X$ for which $\mathrm{ord}_P(\omega) \geq 0$ for all $P \in X$ are called regular.

According to the Proposition 2.23.5 $\mathrm{div}_P(\omega)$ is well defined and the previous lemma gives us a way to calculate the coefficients $\mathrm{ord}_P(\omega)(P)$ in many cases. However, in this thesis we will not have to make such calculations.

Definition 2.28. The *canonical divisor class on* X is the image in $\mathrm{Pic}(X)$ of $\mathrm{div}(\omega)$ for any nonzero differential $\omega \in \Omega_X$. A divisor in the canonical divisor class is called a *canonical divisor*.

We have to be a bit careful. This definition makes sense since Proposition 2.23.1 holds. This follows from the fact that if $\omega_1, \omega_2 \in \Omega_X$ are nonzero differentials, then there is a rational function $f \in \overline{K}(X)^*$ so that $\omega_1 = f\omega_2$ and hence $\mathrm{div}(\omega_1) = \mathrm{div}(f) + \mathrm{div}(\omega_2)$ (remember $\mathrm{div}(f) = (f)$).

Recall (see Definition 2.14) that for a divisor D on a curve X we associated to D a $\overline{K}-$vector space $L(D)$, namely

$$L(D) = \{f \in K(X)^* : (f) + D \geq 0\} \cup \{0\}.$$

The case in which D is a canonical divisor is of special interest:

Let $K_X = \mathrm{div}(\omega) \in \mathrm{Div}(X)$ be a canonical divisor on X where ω is some nonzero differential. By definition each $f \in L(K_X)$ satisfies $\mathrm{div}(f\omega) = \mathrm{div}(f) + \mathrm{div}(\omega) \geq 0$. This means that

$$L(K_X) \simeq \{\omega \in \Omega_X : \omega \text{ is regular}\}.$$

The next theorem is called the Riemann-Roch theorem:

Theorem 2.29. *Let X be a curve and K a canonical divisor on X. There is an integer $g \geq 0$, called the* genus *of X, such that for every divisor $D \in Div(X)$,*

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

Proof. See [11, IV.1]. □

Corollary 2.30.

(1) $l(K_X) = g$.
(2) $\deg(K_X) = 2g - 2$.
(3) *If* $\deg(D) > 2g - 2$, *then:*

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

Proof. See [29, I.5, Corollary 5.5]. □

Remark 2.31.

(1) A divisor D on X is called special if $l(K_X - D) > 0$ and nonspecial otherwise. In the case that D is special $l(K_X - D)$ is called its index of speciality. Note that if $\deg(D) > 2g - 2$, then D is nonspecial.
(2) A curve of genus $g = 0$ is called a rational curve. In this case $|K_X|$ is empty. If the curve has genus $g = 1$ and a rational point on it, then it is called an elliptic curve and we have $|K_X| = 0$. One can deduce that for any point $P \in X$ we have $\dim |P| = 0$ if and only if $g \geq 1$.

Although for a special divisor D it is hard to predict the exact dimension of $l(D)$ (and hence $|D|$) using the Riemann Roch Theorem, it is still possible to give an upper bound for it, just in terms of the degree of D. Clifford's theorem gives us such a bound. First we give some lemmas and introduce the notion of a hyperelliptic curve.

Now we give a sufficient condition for a complete linear system of to be base point free in terms of the genus. The proof is based on an application of the Riemann-Roch theorem.

Lemma 2.32. *Let D be a divisor on a curve X. The complete linear system $|D|$ has no base point if* $\deg(D) \geq 2g$.

Proof. See [11, IV.3, 3.2]. □

Lemma 2.33. *Let D be a divisor on a curve X of genus g. Then D is very ample if and only if for every two points $P, Q \in X$ (including the case $P = Q$) we have:*

$$\dim |D - P - Q| = \dim |D| - 2.$$

If $\deg D \geq 2g + 1$, *then D is very ample.*

Proof. [11, IV.3, 3.2] □

Let us analyze these lemmas with a view towards the definition of a very ample divisor (Definition 2.21) and an embedding (Proposition 2.20). The previous lemma tells us that the linear system$|D|$ of a very ample divisor D on X has the nice properties of separating points and tangent spaces, hence it gives rise to an embedding. A quite interesting case is when $D = K_X$ is a canonical divisor.

Lemma 2.34. *For a curve X of genus $g \geq 2$ the canonical system $|K_X|$ has no base points.*

Proof. Fix a point $P \in X$. We must show that $\dim |K_X - P| = \dim |K_X| - 1 = g - 2$ (Lemma 2.18). Since $g \neq 0$ the curve X is not rational (Remark 2.31) and hence we have $l(P) = 1$. By Riemann-Roch theorem:

$$1 = l(P) = l(K_X - P) + deg(P) + 1 - g = l(K - P) + 2 - g$$

So $l(K_X - P) = g - 1$ and $\dim |K_X - P| = g - 2$. □

Recall that the degree of a finite morphism of curves $f : X \to Y$ is defined as the degree of the field extension $[K(X) : K(Y)]$.

Definition 2.35. A curve X is called hyperelliptic if $g \geq 2$ and there exists a finite morphism $f : X \to \mathbb{P}^1$ of degree 2. We call X nonhyperelliptic if $g \geq 2$ and X is not hyperelliptic.

Example 2.36. If X has genus $g = 2$, then a canonical divisor K_X on X has degree $2g - 2 = 4 - 2 = 2$ and by Riemann-Roch theorem $l(K_X) = 1$. So the complete linear system $|K_X|$ has dimension 1. It has no base points by Lemma 2.34. Hence $|K_X|$ defines a morphism of degree 2 from X to $\mathbb{P}^1$.

Proposition 2.37. *Let X be a curve of genus $g \geq 2$ then $|K_X|$ is very ample if and only if X is not hyperelliptic.*

Proof. See [11, IV.5, Proposition 5.2]. □

Theorem 2.38. *(Clifford's theorem) Let D be an effective special divisor on a curve X. Then*

$$\dim |D| \leq \frac{1}{2}\deg(D).$$

The equality occurs if and only if either $D = 0$ or $D = K_X$ or X is hyperelliptic and D is a multiple of its unique g^1_2.

Proof. See [11, IV.5, Theorem 5.4]. □

2.3. **Hurwitz's Theorem.**

Let $f : X \to Y$ be a finite morphism of curves over K. We give in this subsection a relation between the genus of these two curves which follows from a relation between their canonical divisors.

Let $P \in X$ and let $Q = f(P)$. Let $t_Q \in \mathcal{O}_Q$ be a uniformizer at Q. We can view t as an element of $\mathcal{O}_P$ via the natural map $f^* : \mathcal{O}_Q \to \mathcal{O}_P$. Set $e_P = v_P(t)$ where v_P is the valuation associated to $\mathcal{O}_P$. We see that for a uniformizer $t_P \in \mathcal{O}_P$ we have $f^*(t_Q) = t_P^{e_P} u$ where $u \in \mathcal{O}_P^*$. If $e_P > 1$, then f is said to be ramified at P and in this case Q is called a branch point of f. If $e_P = 1$, then f is called unramified at P. If $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) = p$ but p does not divide e_P the ramification is said to be tame at p. If p divides e_P, then it is called wild at p. The morphism f is called wildly ramified if it has a wild ramification point and it is called tamely ramified if it has only tame ramification points.

We construct an induced homomorphism $f^* : \mathrm{Div}(Y) \to \mathrm{Div}(X)$ by defining

$$f^*(Q) = \sum_{f(P)=Q} e_P P$$

and extending it by linearity. One can check that this definition does not depend on the uniformizers chosen. Note that $\deg f^*(Q) = \deg(f)$ for any point $Q \in Y$ and that $\deg f^*(D) = \deg(D)\deg(f)$ holds for any divisor $D \in \mathrm{Div}(Y)$.
Keeping the notation above we have $f^*(dt_Q) = g dt_P$ for some $g \in \mathcal{O}_P$. Set $b_P = \mathrm{ord}_P(g)$. Then $b_P \neq 0$ only for ramification points of f. We define the ramification divisor of f to be

$$R_f = \sum b_P P \in \mathrm{Div}(X).$$

Using this definition we can state the following theorem:

Theorem 2.39. *Let $f : X \to Y$ be a non-constant separable morphism of degree n. Let $g(X)$ and $g(Y)$ be the genus of X respectively Y. Then*

$$2g(X) - 2 = n(2g(Y) - 2) + \deg(R_f).$$

Proof. See [28, IV, Theorem 33]. Let K_X and K_Y be canonical divisors of X respectively Y. If we show that $K_X = f^*(K_Y) + R_f$, then by taking the degrees and using Corollary 2.30 we find $2g(X) - 2 = n(2g(Y) - 2) + \deg R_f$.
Take $0 \neq \omega \in \Omega_Y$ such that $\mathrm{supp}(\omega)$ is disjoint from the finite set of branch points of f. Let $Q \in Y$ and suppose Q is not a branch point of f and that $\omega = g dt_Q$ where t_Q is a uniformizer at Q. Then $f^*(t_Q)$ is a uniformizer for any point P in the fiber above Q. So K_X and $f^*(K_Y)$ coincide on $X \backslash \mathrm{supp}(R_f)$. Now suppose that Q is a branch point of f and write $\omega = h dt_Q$ for some rational function h. We assumed that $Q \notin \mathrm{supp}(\omega)$ hence $\mathrm{ord}_Q(h) = 0$. Let $P \in X$ such that $f(P) = Q$. Let $f^*(dt_Q) = g t_P$. Then $\mathrm{ord}_P(f^*(\omega)) = \mathrm{ord}_P(g)$ and so $\mathrm{ord}_P(f^*(\omega)) = b_P$, since $ord_P(f^*(h)) = 0$. □

In the case that f has only tame ramification we get the famous Hurwitz's formula:

Corollary 2.40. *Let $f : X \to Y$ be a non-constant separable morphism of degree n which is tamely ramified, then*

$$2g(X) - 2 = n(2g(Y) - 2) + \sum_{P \in X(\overline{K})} (e_P - 1).$$

Proof. According to the previous theorem it suffices to show that $R_f = \sum_{P \in X(\overline{K})}(e_P - 1)$. Keeping using the notation above if $f^*(t_Q) = ht_P^{e_P}$ with $ord_P(h) = 0$, then $f^*(dt_Q) = e_P h t^{e_P - 1} dt_P + t^{e_P} dh$. Since the characteristic of K does not divide e_P we have $e_P \neq 0$ in K and the formula follows. □

2.4. **Gonality.** Now we define the gonality of a curve and state some results on it. We borrow the definition and results from [38, 4.2.25, p. 215].

Definition 2.41. The gonality $\gamma(X)$ of a curve X over a field K is the minimal degree of a non-constant map (defined over K) from X to the projective line.

Lemma 2.42. *If D is a divisor of degree $\deg D < \gamma(X)$, then $l(D) \leq 1$.*

Proof. If $l(D) > 1$, then there exitss a non-constant rational function f on X such that $(f) \geq -D$, whence we have $(f)_\infty \leq D$. One can view f also as a non-constant map, defined over the field of constants, from X to the projective line. The degree of this map is equal to $\deg(f)_\infty \leq \deg D < \gamma$ contradicting the definition of gonality. □

Lemma 2.43. *Let X be a curve of genus g defined over $\mathbb{F}_q$ and let $N = \#X(\mathbb{F}_q)$, then $g + 1 \geq \gamma(X) \geq \frac{N}{q+1}$. Moreover if $\gamma = g + 1 > 3$ then $g \leq 10$ and $q \leq 31$.*

Proof. For the left inequality note that over a finite field there always exists a divisor of degree $g + 1$ (see [21, Theorem 3.2]). By the Riemann-Roch theorem the dimension of such a divisor is at least 2.

For the right inequality note that under a non-constant map of degree γ from a curve X to the projective line, the N rational points of the curve are mapped to one of the $q + 1$ rational points of the projective line and the inverse of a point on the projective line contains at most γ rational points.

Assume now that $\gamma = g + 1 > 3$. We first show that such a curve has no effective divisors of degree $g - 2$. Indeed, if such a divisor D exists, take a canonical divisor K_X so you get $l(K_X - D) \geq l(K_X) - deg(D) = 2$ and $\deg(K_X - D) = g$. So $\deg(K_X - D) = g < g + 1 = \gamma$. But this contradicts Lemma 2.42. Now the curve has no effective divisors of degree $g - 2$ hence the curve over an extension of degree $g - 2$ has no rational points. By the Weil bound we have

$$q^{g-2} + 1 - 2gq^{\frac{g-2}{2}} \leq 0$$

whence $g < 2\log_q(2g) + 1$. This implies that $g \leq 10$ and $q \leq 31$.

□

Lemma 2.44. *Let X be a curve of genus g, then:*

1. *$\gamma(X) = 1$ if and only if X is isomorphic to the projective line.*
2. *$\gamma(X) = 2$ if and only if X is either elliptic or X is hyperelliptic.*

3. MDS codes and finite geometry

In this section we state some results on arcs in projective spaces. These objects are closely related to MDS codes. In fact we will see that the existence of these arcs is equivalent in some sense to the existence of MDS codes.

One notes that in the literature the most important results on arcs and on the main conjecture of MDS codes are stated in the language of 'arcs in projective spaces'. Important works have been done by Segre [25], [26], [27] and later Thas [35], [36], Casse [6], Hirschfeld [14] and others.

Definition 3.1. Let $\mathbb{P}^{k-1}(\mathbb{F}_q)$ be the projective space of $k-1$ dimensions over $\mathbb{F}_q$. A set S of $n \geq k$ points in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ is said to be an $n-$arc if there is no hyperplane containing k points of the set.

The following lemma gives the relation between MDS codes and arcs. It follows easily from Proposition 1.7. It has been used implicitly in Subsection 1.3.

Lemma 3.2. *We have the following one to one correspondence:*

$$\begin{gathered} \{[n,k]\text{-MDS codes over } \mathbb{F}_q\} / \sim \\ \updownarrow \\ \{n\text{-arcs in } \mathbb{P}^{k-1}(\mathbb{F}_q)\} \end{gathered}$$

where $\sim$ denotes the equivalence of linear codes (Section 1.1).

3.1. Complete arcs.

An $n-$arc $\mathcal{A}$ in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ is called complete if it is not contained in any $(n+1)-$arc in $\mathbb{P}^{k-1}(\mathbb{F}_q)$. We denote by $m(k-1,q)$ the maximum size of an $n-$arc in $\mathbb{P}^{k-1}(\mathbb{F}_q)$. We have the following results on $n-$arcs (See [12, Table 3, p.50]):

Theorem 3.3. *For q odd we have: $m(k-1,q) = q+1$ if $q > (4k - \frac{55}{4})^2$.*

Theorem 3.4. *For q even we have: $m(k-1,q) = q+1$ if $q > (2k - \frac{15}{2})^2$.*

Proof. See [37], Theorem E. □

Next we translate these two results into a statement about the main conjecture of MDS codes (Subsection 1.3).

Theorem 3.5. *The main conjecture of MDS codes holds in the following cases:*

1. *For q odd with $q > (4k - \frac{55}{4})^2$.*
2. *For q even with $q > (2k - \frac{15}{2})^2$.*

Proof. This follows directly from Theorems 3.4 and 3.3 and the obvious fact that the maximum length of an MDS code over $\mathbb{F}_q$ of dimension k is equal to the maximum size of an $n-$arc in $\mathbb{P}^{k-1}(\mathbb{F}_q)$. □

Remark 3.6. The proofs of the previous lower bounds for q in terms of k use finite geometries. To get a very good feeling on how these proofs proceed one can have a look at [33] and [24]. The main idea is to find a lower bound in the case of plane arcs. By induction on the dimension of the projective space and using projections a modified bound is proved for higher dimensions.

The next two examples give a feeling about how algebraic geometry and finite geometries come together when dealing with linear MDS codes.

Example 3.7. Consider in $\mathbb{P}^2(\mathbb{F}_q)$ with $q > 2$ the nondegenerate conic given by the equation $x_0^2 = x_1x_2$ where x_i for $i = 0, 1, 2$ are homogeneous coordinates in $\mathbb{P}^2(\mathbb{F}_q)$. This conic consists of $q+1$ ($\mathbb{F}_q$-)rational points: $(0 : 1 : 0)$, $(0 : 0 : 1)$ and $(x : 1 : x^2)$ with $x \in \mathbb{F}_q^*$ and these points lie in general position. We construct a linear code C as follows: take of each of the rational points on the conic one representative. A parity check matrix H of C is a $3 \times (q+1)$-matrix of which the columns are exactly those representatives. Since the points on the conic are in general position, each triple of the columns of H is linearly independent so by Remark 1.2 the minimal distance of C is 4. We see that C is an $[q + 1, q - 2, 4]$ MDS code.

By Lemma 3.2 the points $(0 : 1 : 0)$, $(0 : 0 : 1)$ and $(x : 1 : x^2)$ with $x \in \mathbb{F}_q^*$ form an $(q + 1)$-arc in $\mathbb{P}(\mathbb{F}_q^2)$. Is this arc complete? In other words, can we extend this $(q + 1)$-arc by adding a rational point from $\mathbb{P}(\mathbb{F}_q^2)$ to get an $(q + 2)$-arc? The answer depends on the parity of q. In the case that q is odd Segre [23] proved that $(q + 1)$-arcs are complete. In the case $q > 2$ is even we can extend the $(q + 1)$-arc above by adding the point $(1 : 0 : 0)$ the intersection of all tangent lines of points on the conic, such point is called the nucleus of a conic. A quick verification shows that these $(q + 2)$ points are in general position. So this construction gives us an $[q + 2, q - 1, 4]$ MDS code. Now to see that this $(q + 2)$-arc is complete remember that we have shown in Subsection 1.3 for an MDS code that $n \leq q + 2$ when $k = 3$ and q is even.

Example 3.8. As a generalization of the previous example we show that it is always possible to construct an $(q + 1)$-arc in $\mathbb{P}^m(\mathbb{F}_q)$ with $m \geq 2$. Consider the image X of the embedding

$$v_m : \mathbb{P}^1 \to \mathbb{P}^m$$
$$(x_0 : x_1) \to (x_0^m : x_0^{m-1}x_1 : ... : x_1^m) = (z_0 : ... : z_m).$$

Such a curve is called a rational normal curve. It is the common zero locus of the polynomials $z_iz_j - z_{i-1}z_{j+1}$ for $1 \leq i \leq j \leq m - 1$. As the name v_m may suggest this map is just the well known Veronese map of degree m. Note that in the case $m = 2$ we get $z_1^2 = z_0z_2$ which is just the curve in Example 3.7. If $m = 3$, then we get the well known twisted cubic.

Note that any $m + 1$ points of a rational normal curve as described above are linearly independent. This is due to the fact that the Vandermonde determinant only vanishes if two of its rows coincide.

In general, for q odd it is not known yet whether points of rational normal curves always form a maximal arc. The completeness of rational normal curve has been investigated by Storme, Thas, Kovacs and others. In [32] the problem is solved for the case that q is a large prime number and for the following case proved by Storme:

Theorem 3.9. *For each prime number $p, p \geq 1007231$, every normal rational curve in $\mathbb{P}^n(\mathbb{F}_p)$, $2 \leq n \leq p - 1$, is complete.*

Theorem 3.10. *For a fixed integer $h \geq 1$ let $p_0(h)$ be the smallest odd number p satisfying*

$$p^{h+1} > 24p^h\sqrt{p(2h + 1)ln(p)} + \frac{29}{4}p - 20.$$

Then for each odd prime number $p \geq p_0(h)$ in $\mathbb{P}^n(\mathbb{F}_q)$, $q = p^{2h+1}, 2 \leq n \leq p-1$, every normal rational curve is complete.

4. Translation into algebraic geometric terms

4.1. **Algebraic-geometric codes.**

In Section 3 we translated the 'object' MDS code into an object in (finite) geometry. In this section we give an approach from the point of view of algebraic geometry. For this we restrict our attention to the case of Algebraic Geometric (Goppa) Codes. Notions and tools from Section 2 will be useful. Since we will be working with curves over a finite field $\mathbb{F}_q$, it will be important to know something about the number of $\mathbb{F}_q$-rational points on such curves. The Hasse-Weil bound is an important tool in the proofs of many results on algebraic geometric codes.

Theorem 4.1. *Let X be a curve over $\mathbb{F}_q$ of genus $g \geq 0$. Then we have*

$$|\#X(\mathbb{F}_q) - (q+1)| \leq 2gq^{\frac{1}{2}}.$$

Proof. See [31, VI, Theorem 2.3]. □

Now we define the notion of an algebraic geometric (or Goppa) code:

Definition 4.2. (Goppa 1978)
Let X be a curve over $\mathbb{F}_q$. Let $P_1, ..., P_n \in X(\mathbb{F}_q)$ be n distinct points. Define the divisor $D = P_1 + P_2 + ... + P_n$ on X. Let G be any divisor on X defined over $\mathbb{F}_q$ of which the support is disjoint from the support of D. The Goppa Code $C(X, D, G)$ is the image of the linear map

$$\alpha_G : L(G) \to \mathbb{F}_q^n$$
$$f \mapsto (f(P_1), ..., f(P_n)).$$

Remark 4.3.

(1) According to Lemma 2.15 this definition makes sense because it is possible to give a basis for $L(G)$ consisting of functions in $\mathbb{F}_q(X)$ making α_G well defined. So we see $L(G)$ as a $\mathbb{F}_q$-vector space.
(2) The assumption $\text{supp}(G) \cap \text{supp}(D) = \emptyset$ is in some sense not necessary. One can redefine $C(X, D, G)$ by choosing a $t \in \mathbb{F}_q(X)$ with $\text{ord}_{P_i}(t) =$ multiplicity of P_i in G and sending $f \in L(G-(t))$ to $(f(P_1), ..., f(P_n))$. A different choice of such t gives a different but an equivalent code [6].
(3) If we are interested in the parameters of a code, we may assume without loss of generality that G is effective and we then get is an equivalent code. This follows from the fact that for a divisor G defined over k on a curve X with $l(G) \neq 0$ there exist $G' \geq 0$ such that $G \sim G'$. The proof is easy: $l(G) > 0$ hence there is an $0 \neq f \in L(G)$. By definition $(f) + G \geq 0$ so just take $G' := (f) + G$.

[6]For each $P_i \in D$ let $\phi_i \in \mathbb{F}_q(X)^*$ such that $\text{ord}_{P_i}(\phi_i) = \text{ord}_{P_i}(G)$. Then send f to $(\phi_1 f_1(P_1), ..., \phi_n f_n(P_n))$. If we take another $\psi_i \in \mathbb{F}_q(X)^*$ such that $\text{ord}_{P_i}(\psi_i)$ and we define $\lambda_i = \psi_i/\phi_i$, then λ_i lies in $(F)_q(X)^*$ and has no poles or zeroes at P_i. So choosing ψ_i in stead of ϕ_i leads to a multiplication of the coordinates by nonzero constants $\lambda_i(P_i)$. Hence it gives an equivalent code.

(4) If $C(X, D, G)$ is an $[n, k]$ AG-code defined over $\mathbb{F}_q$, then there exist $P_1, ..., P_n \in X(\mathbb{F}_q)$ and an effective divisor G' of degree $k - 1 + g$ such that $C \sim C(X, P_1 + ... + P_n, G')$.

We list two statements on the parameters of algebraic geometric codes. We inherit the notation of Definition 4.2.

Proposition 4.4. *(Goppa 1978)*
Let k and d be the dimension and the minimum distance of $C(D, G) = C(X, D, G)$. Then we have

(1) $k = \dim L(G) - \dim L(G - D)$. *In particular if $n > \deg(G)$, then $k = \dim L(G)$. If moreover $2g - 2 < \deg(G)$ we have $k = \deg(G) + 1 - g$.*
(2) $d(C(D, G)) \geq n - \deg(G)$.

Proof.

(1) Let $f \in \ker(\alpha_G)$. Then f vanishes in P_i for $i = 1, ..., n$. Since $P_i \notin \operatorname{supp}(G)$ for $i = 1, ..., n$ we must have $f \in L(G - D)$. This gives $C(D, G) \cong L(G)/L(G-D)$ which implies (1). Now if $n > \deg(G)$, then $\dim L(G-D) = 0$ so α_G is injective and hence $k = \dim L(G)$. If moreover $2g - 2 < \deg(G)$, then by the Riemann-Roch theorem $k = \deg(G) + 1 - g$.
(2) There exists an $0 \neq f \in L(G)$ with $w(\alpha_G(f)) = d(C(D, G)) = d > 0$. Without loss of generality we may assume that $f(P_i) \neq 0$ for $i = 1, ..., d$ and $f(P_i) = 0$ for $i = d+1, ..., n$. This means that $0 \neq f \in L(G-P_{d+1}-...-P_n)$. so $\deg(G) - (n - d) = \deg(G - P_{d+1} - ... - P_n) \geq 0$ hence $d \geq n - \deg(G)$.

□

In Section 1 we defined the dual of a linear code. Now we define 'the dual of an algebraic geometric code' and show that it is also an algebraic code arising from the same curve and that it is indeed its dual in the usual sense. We deduce some statements on its parameters and investigate how they are related to the parameters of the original code. For this, Subsection 2.2 is needed. The following and more can be found in [39, 10.6].

Definition 4.5. Let D be a divisor on a curve X over K. We define

$$\Omega(D) := \{\omega \in \Omega(X) : (\omega) - D \geq 0\}.$$

The dimension $\dim_K \Omega(D)$ is the called the index of speciality of D.

Note that we have defined the index of speciality in Remark 2.31. One can see that $\dim_K \Omega(D) = l(K_X - D)$ by noticing that the linear map

$$\phi : L(K_X - D) \to \Omega(D)$$
$$f \mapsto f\omega$$

where ω is a canonical divisor is an isomorphism.

Definition 4.6. Let $C = C(X, D, G)$ denote an algebraic geometric code. The dual algebraic geometric code $C^*(X, D, G)$ is the image of the linear map

$$\alpha^* : \Omega(G - D) \to \mathbb{F}_q^n$$
$$\eta \mapsto (\operatorname{res}_{P_1}(\eta), ..., \operatorname{res}_{P_n}(\eta)),$$

where $\operatorname{res}_{P_i}(\eta)$ is the residue of η at P_i.

Proposition 4.7.

(1) *The code* $C^*(D,G)$ *has dimension* $k^* = \dim L(K_X + D - G) - \dim L(K_X - G)$. *In particular if* $\deg(G) > 2g-2$, *then* $k^* = \dim L(K_X + D - G)$ *and if* $\deg(G) < n$ *also holds, then* $k^* = n - (\deg(G) + 1 - g)$.
(2) *For the minimum distance we have* $d^* \geq \deg(G) - 2g + 2$.

Proof.

(1) The kernel of α^* is $L(K_X - G)$ so if $\deg(G) > 2g-2$ then α^* is injective since $\dim L(K_X - G) = 0$. Using the Riemann-Roch theorem if $2g-2 < \deg(G) < n$ we get $k^* = L(K_X + D - G) = n - (\deg(G) + 1 - g)$.
(2) Imitate the proof for Proposition 4.4.

□

From this proposition we see why it is common to ask for G and D in the definition of $C(X,D,G)$ that $2g-2 < \deg(G) < \deg(D)$: the parameters become easy to calculate. Remark 4.3.4 tells us that if we are interested in the parameters of an AG-code, then it is not a restriction to assume that $2g-2 < \deg(G) < \deg(D)$.

Proposition 4.8. *The codes* $C(X,D,G)$ *and* $C^*(X,D,G)$ *are dual to each other.*

Proof. We first show that $C^* \subset C^\perp$ and then that $\dim C^* = \dim C^\perp$. This gives $C^* = C^\perp$.
Let $\eta \in \Omega(G-D)$ and $f \in L(G)$. We want to show that $\alpha(f) \cdot \alpha^*(\eta) = 0$. We have:

$$\alpha(f) \cdot \alpha^*(\eta) = \sum_{i=1}^{n} f(P_i)\mathrm{res}_{P_i}(\eta).$$

The differential form $f\eta$ lies in $\Omega(-D)$ so $f\eta$ has simple poles only in $\mathrm{supp}(D)$. By the Residues theorem:

$$0 = \sum_{P \in (\overline{K})} \mathrm{res}_P(f\eta) = \sum_{i=1}^{n} \mathrm{res}_{P_i}(f\eta) = \sum_{i=1}^{n} f(P_i)\mathrm{res}_{P_i}(\eta).$$

Hence $\alpha(f) \cdot \alpha^*(\eta) = 0$.
We have

$$\dim C^\perp = n - k = n - \dim L(G) + \dim L(G-D)$$

$$= \dim L(K_X + D - G) - \dim L(K_X - G) = k^* = \dim C^*.$$

We conclude that $C^* = C^\perp$. □

Proposition 4.9. *Let* $C(X,D,G)$ *be an algebraic geometric code such that* $2g-2 < \deg(G) < n$ *and let* $C^*(X,D,G)$ *be its dual. Denote by* d *and* d^* *the minimum distance of* $C(X,D,G)$ *and* $C^*(X,D,G)$ *respectively. Then:*

(1) $n - \deg(G) \leq d \leq n - \deg(G) + g$.
(2) $\deg(G) - 2g + 2 \leq d^* \leq \deg(G) - g + 2$.

Proof. The bounds on the right hand side are the Singleton bound (Remark 1.5). The bounds on the left hand side follow from Propositions 4.4 and 4.7. □

Thinking of AG MDS codes we get the following corollary:

Corollary 4.10. *Suppose that* $2g-2 < \deg(G) < n$. *Then the codes* $C(X,D,G)$ *and* $C^*(X,D,G)$ *are MDS if* $g = 0$.

4.2. **Bound on n.**
In Corollary 1.10 we proved for an $[n,k]$ MDS code over $\mathbb{F}_q$ that $n \leq q+k-1$ using MacWilliam's identity. For the special case where the code is also algebraic geometric we give another proof which makes use of a totally different technique.

Proposition 4.11. *Let $C = C(X, \mathcal{Q}, G)$ be an $[n,k]$-AG MDS code with G a very ample divisor. Then we have*

$$n \leq q + k - 1.$$

Proof. Let $\mathcal{Q} \subset X(\mathbb{F}_q)$ be a set of n rational points on a curve X such that $\mathcal{Q}$ gives rise to an $[n,k]$-AG MDS code $C = C(X, \mathcal{Q}, G)$. So we have $k = l(G)$ and G is disjoint from $\mathcal{Q}$. Define $d = \deg(G)$ and note that G gives rise to an embedding $X \hookrightarrow \mathbb{P}^{k-1}$ and we get $\deg(X) = \deg(G) = d$. By abuse of notation we use $\mathcal{Q}$ and $X(\mathbb{F}_q)$ to denote the image of these sets under the embedding. We wish to give an upper bound for $\#\mathcal{Q}$.

Let $Q_1, .., Q_{k-2} \subset \mathcal{Q}$ be $k-2$ distinct points. Then these points span a subspace $V \cong \mathbb{P}^{k-3}$ of codimension 2 in $\mathbb{P}^{k-1}$. Note that V can not contain more points from $\mathcal{Q}$ for if there is $P \in V \cap (\mathcal{Q} \backslash \{Q_1, ..., Q_{k-2}\})$, then adding any other point from $\mathcal{Q} \backslash \{Q_1, ..., Q_{k-2}, P\}$ we get k points of $\mathcal{Q}$ in the same hyperplane which contradicts the fact that $\mathcal{Q}$ gives rise to an MDS code. Choose a line $L \cong \mathbb{P}^1$ defined over $\mathbb{F}_q$ in $\mathbb{P}^{k-1}$ such that V and L are disjoint. We project X from V on L using the following projection ϕ (also called Lefschetz Fibration): Let $P \in X \backslash V$ and consider the hyperplane $\overline{PV}$ spanned by P and V. The image of P is defined as $L \cap \overline{PV}$. We get a morphism over $\mathbb{F}_q$:

$$\phi : X - \{Q_1, ..., Q_{k-2}\} \to L \cong \mathbb{P}^1.$$

Since L is projective the morphism ϕ extends (Theorem 2.19) to a morphism

$$\overline{\phi} : X \to L.$$

We show that $\overline{\phi}$ is injective on $\mathcal{Q} \backslash \{Q_1, .., Q_{k-2}\}$. Let $Q, Q' \in \mathcal{Q} \backslash \{Q_1, .., Q_{k-2}\}$ be two distinct points and suppose that $\overline{\phi}(Q) = \overline{\phi}(Q')$. By definition of ϕ the set of k points $Q, Q', Q_1, .., Q_{k-2}$ lies in the same hyperplane in $\mathbb{P}^{k-1}$. But this can not happen since $\mathcal{Q}$ gives rise to an MDS code. Now there are $q+1$ rational points on L so by the box principle we conclude that $\#\mathcal{Q} = n \leq k-2+q+1 = q+k-1$. □

Remark 4.12.

(1) The proposition implies that $d_{min}(C) = n - k + 1 \leq q$.
(2) To determine the degree of $\overline{\phi}$ we note that for a point $z \in L$ the fibre of z consists of the intersection of X with the hyperplane belonging to z minus the points $Q_1, .., Q_{k-2}$. Hence

$$\deg(\overline{\phi}) = \text{ degree of } X - (k-2) = \deg(X) - (k-2) = d - k + 2.$$

By Riemann-Roch's Theorem: $k \geq d - g + 1$ so $d \leq k + g - 1$ and $\deg(\overline{\phi}) \leq k + g - 1 - (k-2) = g + 1$. In the case that $d \geq 2g - 1$ we get the equality $\deg(\overline{\phi}) = g + 1$.

4.3. **The main conjecture for algebraic-geometric codes.**

In the next subsections we give an overview of attacks on the main conjecture of MDS codes. First we give a geometric equivalence for a geometric code to be MDS. This proposition has been used by many mathematicians working on this problem like Munuera but also by De Boer, Walker and Chen.
We abuse notation and write a divisor $D = P_1 + ... + P_n$ and we denote its support also by D. Whether D is a divisor or a set should be clear from the context.

Proposition 4.13. *Let $C = C(X, D, G)$ be a Goppa $[n, k]-$code. The code C is MDS if and only if for every $m-$tuple of distinct points $P_1, ..., P_m \in D$, $m = 0, ..., k$ it holds* [7] *that*

$$l(G - P_1 - ... - P_m) = k - m.$$

Proof. (See [10, p. 24, Proposition 1.1]).

($\Rightarrow$): Let $C = C(X, D, G)$ be an MDS Goppa $[n, k]-$code. Let $m \in \{0, ..., k\}$ and let $P_1, ..., P_m \in D$ be m distinct points. By Riemann-Roch theorem we have $l(G - P_1 - ... - P_m) \geq k - m$. If $l(G - P_1 - ... - P_m) > k - m$ then for every $(k - m)-$tuple of distinct points $Q_1, .., Q_{k-m} \in D\backslash\{P_1, ..., P_m\}$ we have $l(G - P_1 - ... - P_m - Q_1 - ... - Q_{k-m}) > 0$. Hence there are nonzero code words that vanish in at least k coordinates which contradicts the assumption that C is MDS.

($\Leftarrow$): Suppose that for every $m-$tuple of distinct points $P_1, ..., P_m \in D$, $m = 0, ..., k$ it holds that $l(G - P_1 - ... - P_m) = k - m$. Then in particular we have $l(G - P_1 - ... - P_k) = 0$ for every $k-$tuple of distinct points $P_1, ..., P_k \in D$. So there is no $0 \neq f \in L(G)$ vanishing at k or more points of D. So each nonzero code word has weight at least $n - k + 1$ and hence C is MDS. □

Remark 4.14.

(1) The proof of this proposition tells us that a code $C(X, D, G)$ is MDS if and only if for all nonzero $f \in L(G)$ we have $f(P) = 0$ for at most $k-1$ distinct $P \in D$.
(2) If $C(X, D, G)$ is MDS and X has genus $g = 0$, then the main conjecture holds definitely. This follows easily from the fact that $\#X(\mathbb{F}_q) \leq q + 1$. The length of such code is thus at most $q + 1$ which is consistent with the bounds in the main conjecture.
(3) We have used MacWilliams identities to show that the weight distribution of an MDS code is completely determined by k and n. Proposition 4.13 implies in fact the same result.

Usually when trying to prove the main conjecture of MDS codes for an algebraic geometric MDS code $C(X, D, G)$ authors restrict them to the case that $n = q + 2$. The idea behind this 'without loss of generality' assumption is easy to understand. First a notation: If $D = P_1 + ... + P_n$ with $P_i \neq P_j$ for all $i, j \in \{1, ..., n\}$, then for a positive integer a we denote by D_a a subdivisor of D consisting of a points. The fact

[7] The case $m = 0$ corresponds with $l(G) = k$.

that truncating an MDS code yields an MDS code can easily seen by remembering that for a generator matrix of an MDS codes it holds that each $k \times k$-minor matrix should be invertible (Proposition 1.7). The fact that truncating an AG-code yields an AG-code follows easily from the definition of an AG-code: instead of evaluating all points in the support of D we restrict to a subdivisor D_a.
Now if there exists a geometric code with $n > q+2$, we can truncate the length to $q+2$ without changing k. Hence if the main conjecture does not hold for geometric MDS codes, then there would exist a geometric MDS code of length $n = q+2$ when $k \neq 1, 3$ and q is even.

4.4. **Munuera's proposition.**

The article of Carlos Munuera [22, 1] in 1992 has been the inspiration for the authors of at least four other articles on geometric MDS codes. In his article he deals with geometric MDS codes arising from curves over $\mathbb{F}_q$ of which the genus is 1 or 2 and when q is large enough.

Let X be a curve over $\mathbb{F}_q$ of genus g, $D = P_1 + ... + P_n \subset X(\mathbb{F}_q)$ where the n points are distinct and let G be a rational divisor on X such that $\deg(G) < n$ and $D \cap \mathrm{supp}(G) = \emptyset$. Then $C = C(X, D, G)$ is just the linear code as we defined in Definition 4.2. Now let $t \in \mathbb{Z}, 1 < t \leq n/2 - 2$. We introduce

$$\mathcal{L}_t(D) = \{P_{i_1} + ... + P_{i_t} | i_j \in \{1, ..., n\}, P_{i_r} \in D, P_{i_r} \neq P_{i_s} \text{ if } r \neq s\}.$$

For each t this is just a set of divisors and we write $\mathcal{L}_t(D)/\sim$ for the quotient set, where $\sim$ is the familiar linear equivalence of divisors. We define the following property:

$\mathcal{L}[X, D, t]$: There exists a class in $\mathcal{L}_t(D)/\sim$ such that for every two distinct points $R, S \in D$, this class has at least one representative $E \in \mathcal{L}_t(D)$ (depending on R and S) satisfying that neither R nor S is in E.

The following proposition, due to Munuera, is an essential ingredient in the proofs in the articles of Munuera and authors who exploited his idea. Because of its importance we include a proof of it:

Theorem 4.15. *If $\#D = n > q+1$ and $\mathcal{L}[X, D, t]$ holds for all $1 < t \leq n/2 - 2$, then there are no $[n, k]-$MDS geometric codes arising from D for $3 < k < q$, except possibly for $k = q-1$ and $n = q+2$.*

Proof. See [22, Proposition 1] and [10, Proposition 1.3].
Let $k = t + 2$. Suppose that $C = C(X, D, G)$ is an $[n, k]$ MDS code with $3 < k$ and $n > q + 1$. The dual of a geometric MDS code is also a geometric MDS code by (Proposition 4.8) so we may assume that $3 < k \leq n/2$. By assumption we know that $\mathcal{L}[X, D, k-2]$ holds, so there is a class $[D]$ in $\mathcal{L}_{k-2}(D)/\sim$ such that for every two points $R, S \in D$ there is a representative $D' \in \mathcal{L}_{k-2}(D)$ of $[D]$ not containing R and S in its support. Let $P_1 + ... + P_{k-2}$ be a representative of $[D]$. For any $P_i \in D$ we have $\#|G - P_1 - ... - P_{k-2} - P_i| \geq 1$ by Proposition 4.13. Let E_i be an effective divisor of degree g such that

$$G - P_1 - ... - P_{k-2} \sim P_i + E_i.$$

We claim that the divisors $\{P_i + E_i\}$ where P_i runs over D are pairwise different. If we prove this claim, then it follows that $n = \#D \leq |G - P_1 - ... - P_{k-2}| = q + 1$ which is a contradiction. So suppose we had $P_i + E_i = P_j + E_j$ for some $i \neq j$. Define $E' = E_i - P_j$ and note that $E' = E_j - P_i$ and $E' \geq 0$. We have thus $E_i = P_j + E'$ and $E_j = P_i + E'$. There is a representative Q of $[D]$ such that $Q = Q_1 + ... + Q_{k-2}$ and $P_i, P_j \neq Q_r$ for $1 \leq r \leq k-2$. Hence we find that

$$G \sim Q_1 + ... + Q_{k-2} + P_i + P_j + E'.$$

This says that there exists a nonzero code word in C with at least k zeroes contradicting Proposition 4.13. □

Theorem 4.15 has been proved to be very useful in proving the main conjecture of MDS codes even it works in just one direction.

Remark 4.16.
The theorem is also a corollary of the following: If $\mathcal{L}[X, D, t]$ holds for some t, $1 < t \leq n/2 - 2$, then the maximal length of a non-trivial algebraic geometric MDS codes of dimension $t + 2$ over $\mathbb{F}_q$ is $q + 1$.

Unfortunately, for large genus g the property $\mathcal{L}[X, D, t]$ can be strong if X is hyperelliptic. The next corollary implies that for $g = 3$ the property $\mathcal{L}[X, D, 3]$ never holds for any set D. For a proof of it we refer to [10, Proposition 2.2]. Recall that for a $P \in X(\mathbb{F}_q)$ there is a unique $Q \in X(\mathbb{F}_q)$ such that $P + Q \in g_2^1$, here g_2^1 is the unique linear system of degree 2 and dimension 1. The g_2^1 gives rise to an involution $\iota : X \to X$ and we have $Q = \iota(P)$. Now define $D_t = \{P_1 + .. + P_t | P_i \in D, P_i \neq P_j, \iota(P_j)\}$, so the support of each element of such a D_t does not contain conjugated pairs.

Proposition 4.17. *Let X be a hyperelliptic curve over $\mathbb{F}_q$ and D a set of rational points on X and suppose that $0 \leq t \leq g$. Then $\mathcal{L}[X, D, t]$ holds if and only if t is even and D contains at least $t/2 + 2$ conjugate pairs.*

Nevertheless, Chen succeeded to prove the conjecture for $g \geq 2$ if q is large enough (See Theorem 4.26).

4.5. **Application to elliptic curves.**

We consider the case where X over $\mathbb{F}_q$ is elliptic . This case has been studied by several mathematicians including Munuera and Walker (see next subsection). We give outlines of their proofs. Note how Theorem 4.15 is used in these cases.

We start with some facts on elliptic curves: The rational points $X(\mathbb{F}_q)$ can be given a composition law $\oplus$ induced by a bijection[8] from the Jacobian of X onto $X(\mathbb{F}_q)$ so $X(\mathbb{F}_q)$ becomes an abelian group. Given a divisor $G = \sum n_P P$ we associate to G the point $G^* = \oplus n_P \cdot P$. Note that $G^* \in X(\mathbb{F}_q)$ if G is rational over $\mathbb{F}_q$. One can prove that for two rational divisors G and G' on X we have $G \sim G'$ if and only if $\deg(G) = \deg(G')$ and $G^* = G'^*$. Each pair of distinct points $Q, Q' \in X(\mathbb{F}_q)$ gives rise to a unique point $P = Q \oplus Q' \in \mathbb{F}_q$. We call $\{Q, Q'\}$ a $P-$pair. In fact two $P-$pairs $\{Q, Q'\}$ and $\{R, R'\}$ we must have either $\{Q, Q'\} = \{R, R'\}$ or

[8]The bijection is not unique. You first have to choose a rational point which becomes the neutral element of the group structure.

$\{Q, Q'\} \cap \{R, R'\} = \emptyset$.

The main idea of Munuera's proof is to prove $\mathcal{L}[X, D, t]$ for $1 < t \leq n/2 - 2$ by showing that for a $P \in X(\mathbb{F}_q)$ there exist enough $P-$pairs in D. For instance, if t is even, then Munuera shows it is enough to prove that there is $P \in X(\mathbb{F}_q)$ such that D contains at least $t/2 + 2$ P-pairs. In fact if $\{Q_1, Q_1'\}, ..., \{Q_{t/2+2}, Q_{t/2+2}'\}$ are such P-pairs, then

$$[E] := [Q_1 + Q_1' + ... + Q_{t/2} + Q_{t/2}'] \in \mathcal{L}_t(D)/\sim .$$

Note that all pairs obtained as sum of $t/2$ P-pairs are actually equivalent to E. This follows easily from $G \sim G'$ if and only if $\deg(G) = \deg(G')$ and $G^* = G'^*$ as stated above.

How can we understand this in a more geometric fashion?

We aim to give the set of P-pairs of a point $P \in X(\mathbb{F}_q)$ a geometric interpretation. Let

$$X \times X \xrightarrow{a} X$$

$$(x, y) \longmapsto x \oplus y$$

denote the addition map on X. Then a factors as following

$$\begin{array}{ccc} X \times X & \xrightarrow{a} & X \\ \downarrow{\scriptstyle \iota} & \nearrow{\scriptstyle \overline{a}} & \\ (X \times X)/\iota & & \end{array}$$

where ι denotes the map

$$X \times X \longrightarrow X \times X$$

$$(x, y) \longmapsto (y, x)$$

which exchanges the factors. By taking the quotient we get a smooth projective surface $(X \times X)/\iota$ which is the symmetric product $X^{(2)}$.

Let $p \in X$ be fixed and write O for the identity element under addition in X. Then obviously $\{P, O\}$ is a P-pair and hence $a^{-1}(P)$ is not empty. Now we show that for any $(x_0, y_0) \in a^{-1}(P)$ we have

$$a^{-1}(\{P\}) = \{(x_0 \oplus q, y_0 \ominus q) | q \in X\}.$$

Let $(x_0, y_0) \in a^{-1}(\{P\})$. For $\supset$ note that $(x_0 \oplus q \oplus y_0 \ominus q) = x_0 \oplus y_o = P$ for any $q \in X$. For $\subset$ take any $(u, v) \in a^{-1}(\{P\})$ there is a unique $q \in X$ with $u = x_0 \oplus q$ and $v = y_0 \ominus q$ namely $q := u \ominus x_0$. Note that $v = P \ominus u = x_0 \oplus y_0 \ominus u = y_0 \ominus q$.

Let $\delta : X \to X$ be the involution $x \mapsto \ominus x$. then we have

$$\begin{aligned}
\overline{a^{-1}(\{P\})} &= \overline{\{(x_0 \oplus q, y_0 \ominus q) | q \in X\}} \\
&= \overline{\{(x_0 \oplus q, y_0 \oplus \delta(q)) | q \in X\}} \\
&\cong \overline{\{q + \delta(q) | q \in X\}} \\
&= |P + O| \\
&\cong \mathbb{P}^1.
\end{aligned}$$

Hence taking P-pairs modulo ι we can identify the quotient with a g^1_2.

An important and somehow surprising result of Munuera is the following:

Proposition 4.18. *If a nontrivial MDS code arises from an elliptic code and it has length $n > q + 1$, then it is a $[6, 3]$ code over $\mathbb{F}_4$ arising from an (unique up to isomorphism) elliptic curve with 9 rational points.*

Proof. See [22, Proposition 3]. □

The proof makes use of the group structure of rational points of an elliptic curve, namely the number of points of order 1 or 2 in $X(\mathbb{F}_q)$. It also uses a result of R. Pellikaan and Liu and Kumar [9]. In Section 5 we give an explicit example of such code.

4.6. **Arcs on curves vs AG-codes.**

In 1996 an article [40] of Judy L. Walker was published on the main conjecture on algebraic geometric MDS codes. In her article she described a new approach to attack this conjecture. She used the geometry of a curve after a specific embedding to prove the conjecture in the case of codes arising from curves of genus 1. This result is just a corollary of her main result which is about the maximum number of points in an arc lying on an elliptic curve.

In Lemma 3.2 we established a one-to-one correspondence between classes of MDS $[n, k]$-codes over $\mathbb{F}_q$ and n-arcs in $\mathbb{P}^{k-1}(\mathbb{F}_q)$. The next proposition rephrases this correspondence in the case of algebraic geometric codes. The statement and the proof are modifications of a result of Judy L. Walker.

Write $n = \#D$. If we take G to be any very ample divisor on X with $\mathrm{supp}(G) \cap \mathrm{supp}(D) = \emptyset$ and $\deg(G) \geq 0$, then $\dim L(G) = k = 1 + \deg(G) + \dim L(K_X - G) - g$ (the Riemann Roch theorem), where K_X is a canonical divisor on X.

Proposition 4.19. *Using the notation of Definition 4.2: There is a one-to-one correspondence:*

$$\begin{array}{c}
\{ \text{ Algebraic geometric } [n,k]\text{-MDS codes } C(X,D,G) \text{ over } \mathbb{F}_q \} / \sim \\
\updownarrow \\
\{ n\text{-arcs in } \mathbb{P}^{k-1}(\mathbb{F}_q) \text{ of which all points lie in } X \}
\end{array}$$

where $\sim$ denotes the equivalence of linear codes.

[9] They give an example of an $[6, 3, 4]-$AG-code arising from the curve $X : y^2z + yz^2 = x^3$ over $\mathbb{F}_4$ which has 9 rational points with $X(\mathbb{F}_4) \cong \mathbb{Z}/3 \times \mathbb{Z}/3$.

Proof. See [40, Section 2].
↑:

Assume that X is embedded as a curve $X \subset \mathbb{P}^{k-1}_{\mathbb{F}_q}$ of degree d and genus $g \geq 0$ with $k \geq 2$ and $d = k - 1 + g - \dim\, L(K - G)$. Let $\{Q_1, ..., Q_n\} = \mathcal{Q} \subset X(\mathbb{F}_q)$ be an $n-$arc and denote by $\mathcal{Q}$ also the divisor $Q_1 + ... + Q_n$. We will show that there is a $[n, k]$ MDS code arising from X and $\mathcal{Q}$.
Let $H.X$ be any hyperplane section. By the approximation theorem [10] there is a divisor G defined over $\mathbb{F}_q$ which satisfies:

(1) $G \sim H.X$
(2) $\text{supp}(G) \cap \mathcal{Q} = \emptyset$.

Then G is a divisor of degree d [11]. Consider the code $C = C(X, \mathcal{Q}, G)$ of length n and dimension $k = 1+d+\dim\, L(K-G)-g$ where K_X is the canonical divisor on X. We know that C is MDS if and only if there is no $0 \neq f \in L(G)$ with $f(Q) = 0$ for k distinct $Q \in \mathcal{Q}$. But if such an f exists, we must have $(f) + G = H'.X$ for some hyperplane H' and H' contains at least k points of $\mathcal{Q}$ because the set of hyperplane sections is a complete linear system on X. But then H' contains at least k points of $\mathcal{Q}$ which is impossible by Remark 4.14 since $\mathcal{Q}$ is assumed to be an $n-$arc.

↓:

Let X be a curve of genus g over $\mathbb{F}_q$ and $D \subset X(\mathbb{F}_q)$ with $\#D = n$. Let G be a very ample divisor. Since G is very ample it defines an embedding $\phi : X \to \mathbb{P}^{k-1}$. By letting $Y = \phi(X)$ and $\mathcal{Q} = \phi(D)$ we have Y is a curve of degree equal to $\deg(G)$. Assume that k points of $\mathcal{Q}$ lie in a hyperplane. Write $\phi = (\phi_0 : ... : \phi_k)$. Since the points of D are not in the support of G the functions ϕ_i are regular at each point of D. To say that k points of $\mathcal{Q}$ lie in a hyperplane is to say that for some $a_0, ..., a_{k-1} \in \mathbb{F}_q$, there are k distinct solutions in D to the equation $a_o\phi_0(P) + ... + a_{k-1}\phi_{k-1}(P) = 0$. Since $f = a_0\phi_0 + ... + a_{k-1}\phi_{k-1} \in L(G)$, by Remark 4.14 the code C can not be MDS.

□

Remark 4.20.

(1) We see from the proof that proving that there is an $[n, k]$-MDS code arising from a given curve X with a very ample divisor G on it is equivalent to proving that when X is embedded in $\mathbb{P}^{k-1}$ as a curve of degree $k+g-\dim\, L(K_X - G)-1$, there are $n-$ $\mathbb{F}_q$-rational points of X in general position.

It was Walker's idea to state and prove the one-to-one correspondence of Proposition 4.19. She used this to prove the following theorem:

Theorem 4.21. *Fix $\delta > \frac{2}{3}$. Then there exists $q_0 = q_0(\delta)$ that can be computed effectively such that if $q \geq q_0$, $m \geq \delta q$ and $X \subset \mathbb{P}^{k-1}$ is a curve of genus one and*

[10] A corollary of the (*weak*) *approximation theorem* proven by Lang states that any divisor class containing a K-rational divisor also contains a K-rational divisor whose support is disjoint from a given finite set. See [17, II, lemma 3.].

[11] The degree of an embedded curve is the degree of a hyperplane section.

degree k defined over $\mathbb{F}_q$ with $k \leq \lfloor \frac{m}{2} \rfloor$, then for any set $\mathcal{Q} \subset X(\mathbb{F}_q)$ of m rational points on X, some k points of $\mathcal{Q}$ must lie in a hyperplane of $\mathbb{P}^{k-1}$.

From the theorem above we deduce the following:

If we take $m = q + 2$ and $q > 19$ in the theorem and use older results [12]. from finite geometries we can deduce:

Corollary 4.22. *The main conjecture on MDS codes holds for all AG-codes arising from elliptic curves.*

We give a sketch of the proof of Theorem 4.21 when k is even since. The other case goes almost similarly.

Take $k-2$ distinct rational points $Q_1, ..., Q_{k-2}$ on X in $\mathcal{Q}$ with $Q_1 + Q_2 \sim ... \sim Q_{k-3} + Q_{k-2} \in g_2^1$. According to the lemma there are at least three other pairs $P + P' \in g_2^1$ with $P, P' \in \mathcal{Q}$ and distinct. One can show that through any point $Q \in \mathcal{Q}' = \mathcal{Q} \setminus \{Q_1, ..., Q_{k-2}\}$ there is a unique hyperplane H_Q through Q and $Q_1, ..., Q_{k-2}$. The hyperplane section $H_Q.X$ is of degree k since X itself has degree k. Note that $H_Q.X - Q - Q_1 - .. - Q_{k-2}$ is an effective divisor of degree 1 on X, hence it is a rational point on X.

The next step to show that $H_Q.X$ is the sum of k distinct points from $\mathcal{Q}$, which actually means that there are k points of $\mathcal{Q}$ lying in H_Q and that is what Theorem 4.21 says.

First we construct a $2:1$ morphism π from X to $\mathbb{P}^1$. Such a morphism will give rise to a g_2^1 on X as noticed before. Fix a copy of $\mathbb{P}^1$ not containing $Q_1, .., Q_{k-2}$ and consider X the $\mathbb{P}^{k-2}$ spanned by $Q_1, .., Q_{k-2}$. Denote by $\overline{X}$ the curve obtained from X by extending scalars to $\overline{\mathbb{F}}_q$. Then the projection away from X to $\mathbb{P}^1$ is the Lefschetz fibration which in this case maps points on $\overline{X}$ which don't lie in X to points on $\mathbb{P}^1$. This projection can be extended uniquely to a morphism $\overline{\pi} : \overline{X} \to \mathbb{P}^1$. Roughly speaking, it sends a point $x \in \overline{X}$ to the unique intersection of the hyperplane determined by X and x with $\mathbb{P}^1$. Walker shows that this morphism is $2:1$ and defined over $\mathbb{F}_q$ hence it comes with an involution i.

Now Walker shows that there exists an $Q \in \mathcal{Q}$ with $i(Q) \in \mathcal{Q}' \setminus Q$ which has as a consequence that $H_Q.X \sim Q + i(Q) + Q_1 + ... + Q_{k-2}$, the sum of k distinct points. To do so, one can consider the cases $Q \in \{Q_1, ..., Q_{k-2}\}$ and $Q \in \mathcal{Q}'$. The second case is more interesting. Walker shows that $i(Q) = Q$ if and only if Q is a ramification point of the induced map $\pi : Y \to \mathbb{P}^1$, here $Y = \overline{X} \setminus \overline{X} \cap V$. The Hurwitz's theorem applied to π; which is proved to be separable, shows that there are at most 4 ramification points. If q is large enough, then an application of the Hasse-Weil bound Theorem 4.1 shows that there must be a $Q \in \mathcal{Q}$ with $i(Q) \in \mathcal{Q}' \setminus Q$.

Remark 4.23.

[12]The proof of the conjecture when $q \leq 11$ can be found in [13] and for $13 \leq q \leq 19$ it can be found in [7]

The whole idea of the proof is to view $H_Q.X$ as a divisor in $\mathrm{Pic}^{n+1}(X(\mathbb{F}_q))$ and by subtracting $Q + Q_1 + ... + Q_{n-1}$ from $H_Q.X$ we get an element in $\mathrm{Pic}^1(X(\mathbb{F}_q))$. To write $H_Q.X$ as a sum of $n+1$ distinct points, we need just one point from $\mathcal{Q}$ which is not in the support of $Q + Q_1 + ... + Q_{n-1}$. Using a property of π we show that such extra point exists.

4.7. **Case X is hyperelliptic.**

In the article of Munuera [22] in which he dealt with elliptic curves, he also proves the main conjecture for codes arising from curves of genus $g = 2$ for q large enough. His attack on this special case of hyperelliptic curves has been generalized by de Boer [10] and Chen [8] in their articles to cover many other hyperelliptic curves of higher genus. The characteristic of all these proofs is again the use of Theorem 4.15 and exploiting the existence of a (unique) [13] g_2^1 for hyperelliptic curves. The core of the proof is generalized in the next subsection but we state some specific results on hyperelliptic curves:

Theorem 4.24. *(By Munuera)*
The main conjecture on MDS codes is true for codes arising from curves of genus 2 *when* $q > 83$.

Theorem 4.25. *(By de Boer)*
The main conjecture on MDS codes holds for $[n,k]-$*codes arising from hyperelliptic curves of genus* g *over* $\mathbb{F}_q$ *with* $g+3 < k < n-g-3$ *if*

$$2^{g+2}\binom{\lceil \frac{q}{2} \rceil + 1}{g+2} > 2(\sqrt{q}+1)^{2g}\lfloor \frac{q+1}{g+1} \rfloor$$

and

$$g \leq \frac{q-8}{4\sqrt{q}+6}.$$

In other words for fixed g there is a q_0 such that for all $q > q_0$ the main conjecture holds for MDS codes arising from hyperelliptic curves of genus g over $\mathbb{F}_q$. A very good improvement of this exponential constant q_0 (it is an expression in terms of $g!$) has been reached by the work of Chen:

Theorem 4.26. *(By Chen)*
The main conjecture on MDS codes is true for codes arising from hyperelliptic curves of genus $g \geq 2$ *over* $\mathbb{F}_q$ *if*

$$q > 8g^2 + 4g + 8 + 8g\sqrt{g^2+g+2}$$

or

$$q < 8g^2 + 4g + 8 - 8g\sqrt{g^2+g+2}.$$

4.8. **A generalization of the hyperelliptic case.**

The previous subsections show that proofs for the main conjecture on AG MDS codes heavily make use of the fact that elliptic curves and hyperelliptic curves admit at least a g_2^1. A possible generalization is to look at curves admitting a g_m^1 for $m \geq 3$. We give a generalization in which we assume that m is prime and co-prime to q.

---

[13] The uniqueness has not been necessary in the proofs.

Theorem 4.27. *There exists a constant $q_0 \in O(g^3)$ such that if $q > q_0$ and $C(X, D, G)$ is an MDS code arising from X, where X is a curve over $\mathbb{F}_q$ of genus $g \geq 3$ which has a prime gonality m with $gcd(m, q) = 1$, then the main conjecture of MDS codes holds for $C(X, D, G)$. In other words for such $C(X, D, G)$ we have $n \leq q + 1$ or $n \leq q + 2$ if q is even and $k \in \{3, q - 1\}$.*

Proof. Let X be a curve over $\mathbb{F}_q$ of genus $g \geq 1$ which has a prime gonality $m \geq 3$ with $gcd(q, m) = 1$, then there exists a morphism ϕ of degree m from X to the projective line. So on X there exists at least one linear system g^1_m of dimension 1; which consists of preimages of the points of the projective line under ϕ. We assume that g^1_m is Galois over $\mathbb{F}_q$. That is, there is an automorphism $\sigma : X \cong X$ of order m defined over $\mathbb{F}_q$ such that $X/ < \sigma > \cong \mathbb{P}^1$. Write N_f for the number of ramification points of f. We know by Hurwitz's formula (Corollary 2.40) that $2g-2 = -2m+\deg(R_f)$ where R_f is the ramification divisor. From $(m, q) = 1$ it follows that that f is tamely ramified. Hence there are (since m is prime) $N_f = 2(g + m - 1)/(m - 1)$ ramification points.

As in the definition of geometric codes, take a subset $D \subset X(\mathbb{F}_q)$ and an effective divisor G such that $C = C(X, D, G)$ is an $[n, k]$-code. We prove $\mathcal{L}[X, D, t]$ for $1 < t \leq n/2 - 2$ by assuming that $n = q + 2$ and $3 < k \leq n/2$. We consider two cases and derive two inequalities and then we show when they not hold.
Case 1: t is multiple of m;

First note that $t + 2 = m(t/m + 2/m) \leq m(t/m + 1)$. Hence it suffices to show that D contains at least $t/m + 1 + 1 = t/m + 2$ effective divisors (representatives) from g^1_m such that none is of the form mQ with $Q \in D$. Suppose that D contains at most $t/m+1$ of such representatives. There are at most N_f divisors of the form mQ in D.

We consider the worst case: For at least $n-m(t/m+1)-N_f$ points, these points appear in conjugates, say $Q+\sigma(Q)+...+\sigma^{m-2}(Q)$ and for each such a $(m-1)$-tuple there is a point Q' in $X(\mathbb{F}_q)\backslash D$ such that $Q + \sigma(Q) + ... + \sigma^{m-2}(Q) + Q' \in g^1_m$. If we write $N_1 = \#X(\mathbb{F}_q)$ then we get:

$$m(t/m+1)+N_f+(n-m(t/m+1)-N_f)+(n-m(t/m+1)-N_f)/(m-1) \leq N_1.$$

Hence

$$n + (n - t - m - N_f)/(m - 1) \leq N_1.$$

Case 2: t is not a multiple of m;
A similar counting argument as in Case 1 shows that it suffices to show that there are at least $(t + 1)/m + 2$ representatives of g^1_m in D. This corresponds to the case when m divides $t - m + 1$. Suppose that D contains at most $(t + 1)/m + 1$ of such representatives. Analogous to Case 1 we get the following inequality

$$n + (n - m((t + 1)/m + 1) - N_f)/(m - 1) \leq N_1.$$

Which gives

$$n + (n - t - m - 1 - N_f)/(m - 1) \leq N_1.$$

Using the assumptions $n = q+2$, $t \leq \lfloor n/2 \rfloor -2$ and $N_1 \leq q+1+2g\sqrt{q}$ (Theorem 4.1) together with the fact that $m \leq g + 1$ (Lemma 2.43) we get for both cases that the inequalities hold only for $q > q_0$ for some $q_0 \in O(g^3)$. We conclude that for $q > q_0$ the property $\mathcal{L}[X, D, t]$ holds and hence (by theorem 4.15)the main conjecture for

MDS codes holds for this particular case of MDS codes which satisfy the conditions in the theorem. □

4.9. **A new result.**
We have seen so far that the main conjecture of MDS codes is solved for AG-codes in the case that $g = 1$. For $g = 2$ Munuera solved it for $q > 83$. Note that the conjecture definitely holds for codes rising from curves of genus $g = 0$ since such curves contain (at most) $q+1$ rational points. For hyperelliptic curves Chen gave quadratic bounds $q_0(g)$ and $q_1(g)$ for q such that the conjecture holds if $q > q_0(g)$ or $q < q_1(g)$.

In this subsection we consider a special case of AG-codes and we improve the lower bounds for q in Theorem 3.5 from quadratic bounds in terms of k to linear bounds in terms of k for a fixed genus g. This is a quite interesting improvement in the bound. What is also interesting is the fact that the proof of this new result does not demand from the curve X (in the definition of $C(X, D, G)$) to have a specific linear system or gonality (note that this was necessary in the case of elliptic and hyperelliptic curves). The only nontrivial requirement is that G must be very ample. But in algebraic geometry it is not strange to demand this because very ample divisors are geometrically 'good' divisors since they give rise to embeddings of curves into projective spaces.

Theorem 4.28. *Let X be a curve over $\mathbb{F}_q$ of genus $g \geq 2$. Let δ be a very ample divisor class on X of degree $d \geq 1$. Assume that $k := \dim L(\delta) \geq 4$. Let $\mathcal{Q} \subset X(\mathbb{F}_q)$ with $\#\mathcal{Q} \geq q+2$. There exist constants $\alpha > 0$ and β depending only on g such that if $q > \alpha k + \beta$, then there is a representative H of δ that contains k distinct points from $\mathcal{Q}$ in its support.*

Before we prove this theorem we state and prove the following result:

Corollary 4.29. *Let D (defined over $\mathbb{F}_q$) be a representative of the divisor class δ on X. Then Theorem 4.28 implies the main conjecture of MDS codes for $C(X, \mathcal{Q}, D)$ if q is odd or if q is even and $k \notin q - 1$.*

Proof. Let D (defined over $\mathbb{F}_q$) be a representative of the divisor class δ on X and consider $C = C(X, \mathcal{Q}, D)$. The very ample divisor D gives rise (see Subsection 2.1.1) to an embedding $f : X \hookrightarrow \mathbb{P}(L(D))^* \cong \mathbb{P}^{k-1}$. Consider $f(\mathcal{Q}) \subset \mathbb{P}(L(D))^*$. Note that $\#f(\mathcal{Q}) = \#\mathcal{Q} \geq q + 2$. There exists an effective divisor H on X defined over $\mathbb{F}_q$ with $H \sim D$ and $Q_1, ..., Q_k \in \mathcal{Q} \cap \text{supp}(H)$. This is equivalent to saying that there is a hyperplane in $\mathbb{P}(L(D))^*$ containing k points of $f(\mathcal{Q})$. Hence C can not be MDS (otherwise $\mathcal{Q}$ would be in general position as follows from Proposition 4.19). But this is what the main conjecture of MDS codes tells in the case that q is odd or q is even and $k \notin q - 1$.

□

Now we give a proof of Theorem 4.28:

Proof. We prove the statement by induction on d, the degree of δ.

Case 1: $d \in [1, ..., 2g - 2]$;

Using the Riemann-Roch theorem we have $l(\delta) - l(K_X - \delta) = d - g + 1$ where K_X is the canonical divisor class of X. Note that $\deg(K_X - \delta) \in [0, ..., 2g - 2]$.

Hence, by Clifford's theorem (Theorem 2.38):

$$l(K_X - \delta) - 1 \leq \frac{2g-2}{2}.$$

Hence

$$l(K_X - \delta) \leq g.$$

This gives

$$\begin{aligned} l(\delta) &= d - g + 1 + l(K_X - \delta) \\ &\leq d - g + 1 + g \leq 2g - 2 - g + 1 + g \\ &\leq 2g. \end{aligned}$$

Case 2: $d \in [2g-1, ..., 4g]$;

We have

$$l(\delta) = k = d - g + 1 \leq 3g + 1.$$

For these two cases it holds that for $d \in [1, ..., 4g]$ we have

$$k - 1 = \dim \mathbb{P}(L(\delta))^* \leq 3g.$$

By Theorem 3.5 and since $3 < k < q-1$ we already know that the main conjecture of MDS Codes holds for $k \leq 3g+1$ if $q > (4(3g+1) - \frac{55}{4})^2 = (12g - \frac{39}{4})^2$.

Case 3: $d \geq 4g+1$; We use Case 1 and 2 to do an induction procedure on d. There are $\begin{pmatrix} \#\mathcal{Q} \\ 2g \end{pmatrix}$ effective reduced divisors of degree $2g$ of which the support lies in $\mathcal{Q}$. So there is a divisor class e of degree $2g$ on X having at least $\left\lceil \begin{pmatrix} \#\mathcal{Q} \\ 2g \end{pmatrix} / h \right\rceil$ of such representatives, where $h = \#\mathrm{Pic}^{2g}(X)$. So we have $\delta - e \in \mathrm{Pic}^{d-2g}(X)$. Since $d - 2g \geq 2g + 1$ we know by Lemma 2.33 that $\delta - e$ is a very ample divisor class. The induction hypothesis (since $l(\delta - e) \geq g + 2 \geq 4$) says that there exists an effective representative H' of $\delta - e$ and $\{Q_1, ..., Q_{d-2g-(g-1)} = Q_{d-3g+1}\} \subset \mathcal{Q}$ such that $H' - Q_1 - ... - Q_{d-3g+1}$ is effective.

We show that there exists a representative E of the class e such that $E = Q'_1 + ... + Q'_{2g}$ and $\mathrm{supp}(E) \cap \{Q_1, ..., Q_{d-3g+1}\} = \emptyset$ with $Q'_i \in \mathcal{Q}$. This would imply that for $H := H' + E \in \delta$ we have $H - E = Q_1 + ... + Q_{d-3g+1}$ and so we are done. We count the number of effective representatives of e that contain Q_1 or Q_2 or...or Q_{d-3g+1}. To count those that contain Q_i we note that the set of effective representatives of e containing Q_i can be mapped injectively into the set of effective representatives of $e - [Q_i]$. Hence the number of effective representatives of e containing Q_i is at most

$$\frac{q^{\deg(e)-g+1-1} - 1}{q-1} = \frac{q^g - 1}{q-1}.$$

Here we use that $\deg(e - [Q_i]) = 2g - 1$ and hence the Riemann-Roch theorem tell us the exact dimension of $e - [Q_i]$ namely $l(e - [Q_i]) = 2g - 1 - (g-1) = g$.

Noticing that $d \geq 4g + 1$ and hence $k - 2g > 0$, there are at most

$$(d - 3g + 1)\frac{q^g - 1}{q-1} = (k - 2g)\frac{q^g - 1}{q-1}$$

effective representatives containing Q_1 or Q_2 or...or Q_{d-3g+1}.
Now we are done if

$$\left\lceil \left(\begin{array}{c} \#\mathcal{Q} \\ 2g \end{array} \right) /h \right\rceil > (k-2g)\frac{q^g-1}{q-1}$$

Claim 4.30. *The inequality*

$$\left\lceil \left(\begin{array}{c} \#\mathcal{Q} \\ 2g \end{array} \right) /h \right\rceil > (k-2g)\frac{q^g-1}{q-1}$$

holds for $q > (2g)!2^{2g-1}(k-2g) + 2g(2g-2)$.

Proof. We estimate h using the bound for the Jacobian (Proposition 2.13): $h \leq (\sqrt{q}+1)^{2g} \leq (2\sqrt{q})^{2g} = (4q)^g$ and hence $\frac{1}{h} \geq \frac{1}{(4q)^g}$.
Also

$$\left\lceil \left(\begin{array}{c} \#\mathcal{Q} \\ 2g \end{array} \right) /h \right\rceil \geq \left(\begin{array}{c} \#\mathcal{Q} \\ 2g \end{array} \right) /h \geq \left(\begin{array}{c} q+2 \\ 2g \end{array} \right) /h.$$

Assuming $q+2-2g \geq 1$ (i.e, $q \geq 2g-1$) we get

$$\left(\begin{array}{c} q+2 \\ 2g \end{array} \right) = \frac{(q+2)!}{(2g)!(q+2-2g)!}$$

$$= \frac{(q+2)(q+1)...(q+3-2g)}{(2g)!} > \frac{(q+2-2g)^{2g}}{(2g!)}.$$

On the other hand:

$$\frac{q^g-1}{q-1} < \frac{q^g}{q-1} \leq \frac{q^g}{\frac{q}{2}} = \frac{q^{g-1}}{2}.$$

Combining the results above we see that a solution of

$$\frac{(q+2-2g)^{2g}}{(2g)!(4q)^g} > (k-2g)\frac{q^{g-1}}{2}$$

will give us a solution to Claim 4.30. We solve thus

$$q(\frac{q+2-2g}{q})^{2g} > \frac{(2g)!4^g}{2}(k-2g).$$

Using Bernoulli's inequality (note that $2g$ is even) we get:

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

So

$$q(\frac{q+2-2g}{q})^{2g} \geq q + 2g(2-2g).$$

A solution for q of the inequality

$$q + 2g(2-2g) > \frac{(2g)!4^g}{2}(k-2g)$$

is a solution of the inequality in the claim. Hence for $q > (2g)!2^{2g-1}(k-2g) + 2g(2g-2)$ the claim holds.

□

From the induction basis we see that for $q > (12g - \frac{39}{4})^2$ the main conjecture of MDS codes holds. Combining this with the inequality $q > (2g)!2^{2g-1}(k-2g) + 2g(2g-2)$ there are constants $\alpha(g) > 0$ and β that take in account that $q > (12g - \frac{39}{4})^2$ such that Theorem 4.28 holds. □

5. Examples of AG-codes

Example 5.1.
Let X be the curve over $\mathbb{F}_4$ defined by the equation $y^2z^3 + yz^4 = x^5 + x^3z^2 + xz^4$. Then X has genus 2 and hence is hyperelliptic. Take $G = P_\infty = (1 : 0 : 0)$ and let P be any point of X. Define $G = P + 3P_\infty \in \mathrm{Div}(X)$. Set $D = X(\mathbb{F}_4)\backslash\{P, \sigma(P), P_\infty\}$, where σ is the hyperelliptic involution on X induced by the unique g_2^1 on X. We have $l(G) = l(K - G) + \deg(G) - g + 1 = 0 + 4 - 2 + 1 = 3$. For any P which is not P_∞ we can verify that $C = C(X, D, G)$ is a $[6, 3, 4]$-code and hence it is an MDS code. We use Magma to construct an explicit example of such code by choosing $P := (1 : \alpha : 1)$ with $\alpha \in \mathbb{F}_4^*$ is a primitive generator of the cyclic group $\mathbb{F}_4^*$:

```
> K<x>:= PolynomialRing(GF(4));
> K;
Univariate Polynomial Ring in x over GF(2^2)
> C:= HyperellipticCurve(x^5+x^3+x,1);
> C;
Hyperelliptic Curve defined by y^2 + y = x^5 + x^3 + x over GF(2^2)
> PointsAtInfinity(C);
>{@ (1 : 0 : 0) @}
> pts:=Points(C);
> pts;
{@ (1 : 0 : 0), (1 : $.1 : 1), (1 : $.1^2 : 1), ($.1 : 0 : 1), ($.1 : 1 : 1),
($.1^2 : 0 : 1), ($.1^2 : 1 : 1), (0 : 0 : 1), (0 : 1 : 1) @}
> Involution(pts[1]);
(1 : 0 : 0)
> Involution(pts[2]);
(1 : $.1^2 : 1)
> plcs:=Places(C,1);
> plcs;
[
    Place at (1 : 0 : 0),
    Place at (0 : 0 : 1),
    Place at (0 : 1 : 1),
    Place at ($.1 : 0 : 1),
    Place at ($.1 : 1 : 1),
    Place at ($.1^2 : 0 : 1),
    Place at ($.1^2 : 1 : 1),
    Place at (1 : $.1 : 1),
    Place at (1 : $.1^2 : 1)
]
> SetVerbose("AGCode",true);
> c:=AGCode(plcs[2..#plcs-2],plcs[#plcs-1]+3*plcs[1]);
Algebraic-geometric code:
    Genus computation time: 0.000
    Riemann-Roch dimension: 3
    Riemann-Roch space time:  0.000
    Evaluation time: 0.000
Algebraic-geometric code time: 0.000
> c;
```

```
[6, 3, 4] Quasicyclic of degree 2 Linear Code over GF(2^2)
Generator matrix:
[    1     0     0   $.1     1   $.1]
[    0     1     0   $.1   $.1     1]
[    0     0     1     1   $.1   $.1]
```

Constructing an algebraic geometric hexacode.

Note that Magma writes \$.1 for α.

Example 5.2. (see [39, Example 10.7.6 ,p.164]).
Let $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ and let X be the curve over $\mathbb{F}_4$ defined by $x^2y+\alpha y^2z+\alpha^2z^2x = 0$. Then X has genus 1 and $\#X(\mathbb{F}_4) = 9$. The rational points are given by:

	P_1	P_2	P_3	P_4	P_5	P_6	Q_1	Q_2	Q_3
x	1	0	0	1	1	1	α	1	1
y	0	1	0	α	α^2	1	1	α	1
z	0	0	1	α^2	α	1	1	1	α

Now we construct an algebraic geometric code as follows: Let $D := P_1 + ... + P_6$, $G := 2Q_1 + Q_2$ and consider $C := C(X, D, G)$. The minimal distance d of C is at least $n-\deg(G) = 6-3 = 3$. For the dimension of C we can show that $k = l(G) = 3$ using Riemann Roch's theorem. An explicit method goes as follows: The functions $x/(x + y + \alpha^2z), y/(x + y + \alpha^2z)$ and $\alpha^2z/(x + y + \alpha^2z)$ form a basis of $L(G)$, namely the numerators in these functions are not 0 in Q_1 and Q_2 and the line with equation $x + y + \alpha^2z = 0$ meets X in Q_2 and it is tangent to X in Q_1.

We use Magma to construct the code mentioned after Proposition 4.18 and verify its parameters:

```
>F<w>:=GF(4);F;
Finited field of size 2^2

>K<x,y,z>:=PolynomialRing(F,3);K;
Polynomial ring of rank 3 over GF(2^2)
Order: Lexicographical
Variables: x, y, z

>f:=x^2*y+w*y^2*z+w^2*z^2*x;
>C:=Curve(ProjectiveSpace(k,2),f);C;
Curve over GF(2^2) defined by
$.1^2*$.2+w*$.2^2*$.3+w^2*$.1*$.3^2

>plcs:=Places(C,1);plcs;
[
    Place at (0 : 1 : 0),
    Place at (0 : 0 : 1),
    Place at (1 : 0 : 0),
    Place at (w^2 : w : 1),
    Place at (1 : w : 1),
    Place at (w : w^2 : 1),
```

```
    Place at (w^2 : w^2 : 1),
    Place at (1 : 1 : 1),
    Place at (w : 1 : 1)
]
>l:=[5,7,9] \\ We define a set existing of positions of points in
             \\complement of support of D.
>  m:=1;k:=[]; for i:=1 to #plcs do if i  notin l then k[m]:=plcs[i];
    m:=m+1; end if; end for;
 \\ We define a set called k of points in complement of support of D,
>Div:=DivisorGroup(C);
Group of divisors of Curve over GF(2^2) defined by
$.1^2*$.2 + w*$.2^2*$.3 + w^2*$.1*$.3^2

> G:= Div! plcs[5]+plcs[5]+plcs[9];G;
Divisor 2*Place at (1 : w : 1) + 1*Place at (w : 1 : 1)

>SetVerbose("AGcode",true);
>c:=AGCode(k[1..#k],G);c;

Algebraic-geometric code:
    Genus computation time: 0.000
    Riemann-Roch dimension: 3
    Riemann-Roch space time:  0.000
    Evaluation time: 0.000
Algebraic-geometric code time: 0.000
[6, 3, 4] Linear Code over GF(2^2)
Generator matrix:
[  1   0   0 w^2 w^2   1]
[  0   1   0 w^2   1 w^2]
[  0   0   1   1 w^2 w^2]
```

Hexacode from an elliptic curve.

We see now that $d = 4$ and hence C is MDS.

We can also use Magma to find the algebraic geometric dual code C^* of C:

```
 > AlgebraicGeometricDualCode(k[1..#k], G);
Algebraic-geometric code:
    Genus computation time: 0.000
    Riemann-Roch dimension: 3
    Riemann-Roch space time:  0.010
    Evaluation time: 0.000
Algebraic-geometric code time: 0.010
[6, 3, 4] Linear Code over GF(2^2)
Generator matrix:
[  1   0   0   w   w   1]
[  0   1   0   w   1   w]
[  0   0   1   1   w   w]
```

The dual of a hexacode from an elliptic curve.
It is a self-dual code.

References

[1] A. Aguglia, L. Giuzzi, G. Korchmaros, *Algebraic curves and maximal arcs*, J. Alg. Comb., Volume 28, Issue 4, December 2008.

[2] E. Arbarello, M. Cornalba, P.A. Griffiths, J.Harris, *Geometry of algebraic curves, Volume I*,Springer Verlag, 1984.

[3] Simeon Ball, *On large subsets of a finite vector space in which every subset of basis size is a basis.* To appear in: Journal of the European Mathematical Society (JEMS).

[4] Martin Bright, *The Picard group*, online notes: (http://www.warwick.ac.uk/ maseap/arith/notes/picard.pdf), 2008.

[5] K. A Bush, *Orthogonal arrays of index unity*, Ann. Math. Stat., 23 (1952), 426 − 434.

[6] L.R.A Casse and D.G Glynn, *A solution to Beniamino Segre's " Problem I" for q even*, Att. Accad. Naz. Lincei, Rend. Cl. Sc. Fis. Mat. Natur., 46 (1969) 13 − 20.

[7] J.M. Chao and H. Kaneta, *Rational arcs in $PG(r, q)$ for $11 \leq q \leq 19$*, preprint.

[8] Hao Chen, *On the Main Conjecture of Geometric MDS Codes*, International Mathematics Research Notices, N. 8, 313 − 318, 1994.

[9] Hao Chen, *Contribution to Munuera's Problem on the Main Conjecture of Geometric Hyperelliptic MDS Codes*, IEEE V. 43, N. 4, 1349 − 1354, July 1997.

[10] M. de Boer, *MDS codes from hyperelliptic curves*, on pages 23 − 34 of *Arithmetic, Geometry and Coding Theory*, Walter de Gruyter, 1996.

[11] Robin Hartshorne, *Algebraic Geometry*, 2000, Graduate texts in mathematics: 52.

[12] J.W.P Hirschfeld, *The Main Conjecture for MDS Codes*, Lecture Notes in Computer Science, 1995, Volume 1025/1995, 44 − 52.

[13] J.W.P Hirschfeld and J. A Thas, *General Galois Geometries*, Oxford University Press, Oxford 1991. 44 − 52.

[14] J. W. P Hirschfeld *Rational curves on quadrics over finite fields of characteristic two*, Rendiconti di Matematica, 3 (1971) 772 − 795.

[15] W. Cary Huffman, Vera Pless, *Fundamentals of Error-Correcting codes*, Cambridge University Press 2003.

[16] T.J Kluck, (Master Thesis) *Basic topics in algebraic curve theory*, 2008, (http://www.science.uva.nl/onderwijs/thesis/centraal/files/f1372104392.pdf), p.20

[17] S. Lang, *Abelian varieties*,Interscience Publishers, New York, 1959.

[18] G. Lachaud, M. Martin-Deschamps. *Nombre de points des jacobiennes sur un corps fini.* Acta Arith. 16 (1990), 329 − 340.

[19] F.J. MacWilliams, N.J.A Sloane, *Theory of Error-correcting Codes, Part I*, North Holland Mathematical Library, Vol. 16.

[20] Todd K. Moon: *Error Correction Coding: Mathematical Methods and Algorithms*, John Wiley and Sons, Inc., 2005.

[21] C.J. Moreno, *Algebraic curves over finite fields*, Cambridge Texts in Math. 97, Cambridge University Press, Cambridge, 1991.

[22] Carlos Munuera, *On the Main Conjecture on Geometric MDS Codes*, IEEE V. 38, N. 3, 1573 − 1577, May 1992.

[23] B. Segre: *Ovals in a finite projective plane*,Canadian J. Math., 7 (1955), 414 − 416.

[24] B. Segre, *Introduction to Galois geometries*, Atti Accad. Naz. Lincei Mem. 8 (1967), 133−236. (Edited by J.W.P. Hirschfeld).

[25] B. Segre, *Curve razionali normali e k-archi negli spazi finiti*, Ann. Mat. Pura. Appl., 39, (1955), 357 − 379.

[26] B. Segre, *Le geometrie di Galois*, Annali di Mat., 48, (1959), 1 − 97.

[27] B. Segre, *Lectures on Modern Geometry*, (Edizioni Cremonese, Rome, 1961).

[28] Sergeĭ A. Stepanov, *Codes on algebraic curves*, Kluwer Academic/ Plenum Publishers, 1999.

[29] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer Graduate Texts in Mathematics 106, 1991.

[30] R. C. Singleton, *Maximum distance $q-nary$ codes*, IEEE Trans. Info. Theory, 10 (1964), 116 − 118.

[31] Hennig Stichtenoth, *Algebraic Function Fields and Codes*, First Edition, Graduate Texts in Mathematics 254, 1993.

[32] L. Storme, *Completeness of Normal Rational Curves*, Journal of Algebraic Combinatorics 1 (1992), 197 − 202.

[33] J. A Thas, *Normal rational curves and k-arcs in Galois spaces*, Rendiconti di Matematica, $3-4$, Vol 1., 1968.

[34] J. A Thas, *Complete arcs and algebraic curves in* $PG(2,q)$, J. Algebra 106 (1987) $451-464$.

[35] J. A Thas, *Normal rational curves and k-arcs in Galois spaces*, Rendiconti di Matematica, I (1968) $331-334$.

[36] J. A Thas, *Normal rational curves and* $(q+2)$*-arcs in Galois* $S_{q-2,q}(q=2^h)$, Atti. Accad. Naz. Lincei. Rend. Cl. Sc. Fis. Mat. Natur. (8) 47 (1969) $115-118$.

[37] J.A Thas and L. Storme , *M.D.S codes and arcs in* $PG(n,q)$ *with q even: An improvement of the bounds of Bruen, Thas and Blokhuis*. J. Combinatory Theory Series A 62 (1993), $139-154$.

[38] Michael Tsfasman, Serge Vlăduţ, Dmirty Nogin, *Algebraic Geometry Codes: Basic Notions* , Mathematical Surveys and Monographs, American Mathematical Society, Volume 139.

[39] van Lint J.H: *Introduction to coding theory*, 3d version, Springer, 1999.

[40] Judy L. Walker, *A New Approach to the Main Conjecture on Algebraic-Geometric MDS Codes*, Designs, Codes and Cryptography, 9, $115-120$, 1996.