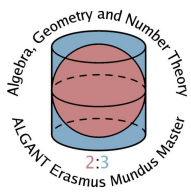
Algebraic geometric codes on curves and surfaces

Paolo Zampolini

Master Program in Mathematics
Faculty of Science
University of Padova,
Italy.

Supervisor: prof. Luca Barbieri Viale

Department of Pure and Applied Mathematics,
University of Padova.
Italy



Padova, 22nd March 2007

"The main application of Pure Mathematics is to make you happy"

H.W. Lenstra, Leiden, November 2005

Contents

Introduction **6**

1 Basic notions of coding theory **7**

2 Algebraic geometric codes on curves **11**
2.1 AG codes 11
2.2 Dual AG codes 12
2.3 Rational points on curves and lower bounds 15

3 Decoding methods **21**
3.1 SV-algorithm 21
3.2 A cubic curve 24
3.3 The Duursma algorithm 27
3.4 Example 34
3.5 Another example: the Klein quartic 36

4 Codes over higher dimensional varieties **41**
4.1 Sheaves of modules 41
4.2 Divisors 45
4.3 Definition of AG codes on varieties 48

5 Codes on surfaces **50**
5.1 Ample and very ample invertible sheaves 50
5.2 Arithmetic and geometric genus of varieties 51
5.3 Basic properties of surfaces 54
5.4 Parameters of codes on surfaces 56

6 Codes on ruled surfaces **59**
6.1 The projective space bundle 59
6.2 Ruled surfaces 60
6.3 Parameters of codes on ruled surfaces 63
6.4 Codes on rational ruled surfaces 64
6.5 Computing the dimension in the decomposable case 65
6.6 Computing the dimension in the general case 66
6.7 Ruled surfaces over elliptic curves 70
6.8 Conclusion and open problems 75

Introduction

One of the main developments in the coding theory in the '80s was the introduction of algebraic geometric codes, due to the russian mathematician and engineer Goppa. His main idea was to associate linear codes to divisors on curves.

In 1982 Tsfasman, Vladut and Zink used this new class of codes to prove the existence of codes with better parameters than the ones ensured by the Gilbert-Varshamow bound.

The theory of algebraic geometric codes on curves has been deeply studied during the '80s and the '90s and now we can consider it to be well-known by the mathematical community. Nowadays most of the works about algebraic geometric codes on curves concern the search of a faster decoding algorithm. Indeed at the present times other codes with more efficient decoding algorithms are preferred to algebraic geometric codes in the applications.

In 1991 Tsfasman and Vladut generalized Goppa's idea and defined algebraic geometric codes on varieties.

Nevertheless, the first publication about codes on higher dimensional varieties is dated 2001. Hansen's PhD thesis opened a new interesting research field, combining both coding theory and the geometry of varieties.

The aim of this work is to introduce the theory of algebraic geometric codes on curves and present the recent progresses about codes on higher dimensional varieties.

In the first section we recall the elementary notions of coding theory.

The second section regards algebraic geometric codes on curves with particular attention to the connection between them and the Gilbert-Varshamov bound, while the third one contains two decoding algorithms for codes on curves.

We introduce in the fourth section codes on higher dimensional varieties and then we follow Hansen and Zarzar's works to study codes on surfaces.

Lastly we focus on Lomont's PhD thesis about codes on ruled surfaces and we try to solve a problem left open in it.

In sections 2 and 3 the language of classical algebraic geometry is assumed to be known, while in the last three sections we also recall the required notions of scheme theory. Proofs are often omitted but we try to define almost every geometric object we use.

1 Basic notions of coding theory

Definition 1.1 *Let $\mathbb{F}_q$ be a field with q elements. An **error correcting code** is a subset C of $\mathbb{F}_q^n$. C is said **linear** if it is a sub-vector space of $\mathbb{F}_q^n$.*

In practice most of the codes are linear codes and they are used to transform words of length $k < n$ (with letters in the alphabet $\mathbb{F}_q$) to words of length n in order to find and correct errors happened during the transmission. The elements of the code are called **words**.

Let x,$y \in \mathbb{F}_q^n$. The **Hamming distance** (or, simply, distance) is defined as

$$d(x, y) := \#\{i \mid 1 \leq i \leq n, x_i \neq y_i\}.$$

d really defines a metric on $\mathbb{F}_q^n$. The **minimum distance** d of a code C is

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

It is immediate to see that the minimum distance of a linear code corresponds to the **minimum weight**

$$w = w(C) := min\{wt(x) \mid x \in C, x \neq 0\},$$

where $wt(x) := \#\{i \mid x_i \neq 0\}$. Let us indicate with (n, M, d) a code of length n, M words and distance d, while an $[n, k, d]$-code is a linear code of length n, dimension k and distance d.

The decoding of a message respects the so-called maximum-likelihood-decoding principle, i.e. we suppose that, during the transmission, the smallest number of errors occurred. The received vector $y \in {\mathbb{F}_q}^n$ is interpreted as the code word $x \in C$ such that $wt(x - y)$ is as small as possible. Thus it is clear that a code with minimum distance d is able to find every error of weight $e < d$ and correct every error of weight not bigger than $e = \lfloor \frac{d-1}{2} \rfloor$. It follows trivially from the triangular inequality that spheres of radius e and center in a code word are disjoint. A code with distance $d = 2e+1$ is said to be **perfect** if such spheres cover $\mathbb{F}_q^n$. Hence, for a perfect code, every $y \in \mathbb{F}_q^n$ has distance less or equal e from a unique code word.

The most immediate relation between the parameters of a code is called singleton bound.

Proposition 1.1 (Singleton bound) *Let C be an $(n, M, d)-$code. Then $Mq^{d-1} \leq q^n$.*

The proposition can be proved just by counting the elements of $\mathbb{F}_q^n$ that belong to the disjoint spheres of radius $e = \lfloor \frac{d-1}{2} \rfloor$ and with a code word as

center. A code whose parameters satisfy the equality in the previous proposition is called **MDS** (maximum-distance-separable). We remark that, for a $[n, k, d]$-code, the singleton bound can be written as $d + k \leq n + 1$.

A fundamental role in the development of coding theory is due to Shannon's work ([20]) and, in particular, to his famous theorem. Suppose we have to transmit a message through a channel where the probability of receiving a wrong digit is p and the probability of transmitting a wrong symbol is the same for every symbol (such a channel is called **uniform**). Furthermore suppose we use a code C formed by M words $x_1, \cdots, x_M$ which occur with the same probability. Let P_i be the probability of not being able to decode exactly x_i according to the maximum-likelihood-decoding principle. In this case the average probability of wrongly decoding a code in C is $P_C = \sum_{i=1}^{n} \frac{P_i}{M}$. Hence a code with good properties is a a code such that P_C is minimum. Let $P^*(M, n, p)$ be the minimum P_C for C running over all the (M, n)-codes and $R = \frac{\log_q M}{n}$ the so-called **information rate**.

Theorem 1.1 (Shannon) *There exists a function c, called **channel capacity**, depending only on q and p, such that, if $0 < R < c$ and $M_n = q^{\lfloor Rn \rfloor}$, then $\lim_{n \to +\infty} P^*(M_n, n, p) = 0$.*

By Shannon's theorem, for R in an interval depending only on the transmission channel, among the codes with the same information rate, the good ones are those with n big. This is a good motivation to look for long codes and to study the asymptotical behavior of codes in the same class, letting n change.

During the transmission of a word of length n through a channel with probability p, we expect an average of pn errors. Hence we need a code with minimum distance $d > 2pn$. We therefore require that d grows at least proportionally to n.

Let $\delta = \frac{d}{n}$, $A_q(n, d) = \max\{M \mid \text{there exists a } (n, M, d)\text{-code over } \mathbb{F}_q\}$. We now define the function α:

$$\alpha(\delta) = \limsup_{n \to +\infty} \frac{\log_q A_q(n, \lfloor \delta n \rfloor)}{n},$$

which is an important and widely studied object of the coding theory. Thus we are interested in studying, for a fixed δ, what the best possible information rate for a code of length n is, and then letting n go to infinity, as suggested by Shannon's theorem. The easiest (and the least precise) among those upper bounds for α is a direct consequence of singleton bound.

Theorem 1.2 *For $\delta \in [0, 1]$, we have $\alpha(\delta) \leq 1 - \delta$.*

Proof: From proposition 1.1 we have $M \leq q^{n+1-d}$ for every (n, M, d)-code, so $A_q(n, \delta n) \leq n+1-\delta n$. Taking the limsup, we conclude that $\alpha(\delta) \leq 1-\delta$.

A much more interesting result is Gilbert's (or Gilbert-Varshamov) lower bound. Define on $[0, \frac{q-1}{q}]$ the entropy function as

$$H_q(x) := \begin{cases} 0 & \text{if } x = 0 \\ x \log_q(q-1) - x \log_q x - (1-x) \log_q(1-x) & \text{if } 0 < x \leq \frac{q-1}{q} \end{cases}$$

H_q is an increasing function and its value in 1 is $\frac{q-1}{q}$. Moreover, define as $V_q(n, d)$ the cardinality of a sphere of radius d in $\mathbb{F}_q^n$ and recall that $V_q(n, d) = \sum_{i=0}^{d} \binom{n}{i} (q-1)^i$.

Lemma 1.1 *For $0 \leq \delta \leq \frac{q-1}{q}$ we have $\limsup_{n \to +\infty} \frac{\log_q V_q(n, \lfloor n\delta \rfloor)}{n} = H_q(\delta)$.*

Proof: The largest addend of $V_q(n, d)$ is $\binom{n}{\lfloor \delta n \rfloor} (q-1)^{\lfloor \delta n \rfloor}$. Therefore

$$\binom{n}{\lfloor \delta n \rfloor} (q-1)^{\lfloor \delta n \rfloor} \leq V_q(n, \lfloor \delta n \rfloor) \leq (1 + \lfloor \delta n \rfloor) \binom{n}{\lfloor \delta n \rfloor} (q-1)^{\lfloor \delta n \rfloor}.$$

We conclude, by taking logarithms, dividing by n and using Stirling formula. □

Lemma 1.2 *For $n \in \mathbb{N}$, $d \in \mathbb{N}$, $q \geq 2$, we have $A_q(n, d) \geq \frac{q^n}{V_q(n, d-1)}$.*

Proof: Let C be a maximal code of length n and distance d. Assume that there exists an element $x \in {\mathbb{F}_q}^n \setminus C$ with distance greater or equal d from every word in C. Then $C \cup \{x\}$ is a code of length n and minimum distance d, contradicting the maximality of C. Hence the spheres of radius $d-1$ and center in C cover ${\mathbb{F}_q}^n$. Thus $|C| V_q(n, d-1) \geq q^n$. □

It can be proved that the previous lemma still holds even if, to calculate $A_q(n, d)$, we consider just linear codes.

Theorem 1.3 (Gilbert) *If $0 \leq \delta \leq \frac{q-1}{q}$, then $\alpha(\delta) \geq 1 - H_q(\delta)$.*

Proof: From previous lemmas we get

$$\alpha(\delta) = \limsup_{n \to +\infty} \frac{\log_q A_q(n, d)}{n} \geq \limsup_{n \to +\infty} \frac{\log_q q^n - \log_q V_q(n, \lfloor \delta n \rfloor - 1)}{n} \geq$$

$$\geq \limsup_{n \to +\infty} \frac{n - \log_q V_q(n, \lfloor \delta n \rfloor)}{n} = 1 - H_q(\delta).$$

□

Even if the lower bound in theorem 1.3 is not optimal, the existence of codes

with better parameters was proved just in 1982 by Tsfasman, Vladut and Zink. They improved the lower bound of theorem 1.3 for $q \geq 49$. It was one of the first important theoretical results obtained by studying algebraic geometric codes.

Let us go back quickly to linear codes. We can associate to an $[n, k]$-code C a $k \times n$ matrix G, called **generator matrix**, where every row is an element of a basis for C. Then $C = \{aG \mid a \in {\mathbb{F}_q}^k\}$. We say that G is written in a **canonical form** if $G = \begin{pmatrix} I_k & P \end{pmatrix}$.

Definition 1.2 *Two codes C_1 and C_2 of length n are said to be **equivalent** if there exists a permutation $\sigma \in S_n$ such that $C_1 = g_\sigma C_2$, where g_σ is the automorphism of $\mathbb{F}_q^n$ which sends $(x_1 \cdots x_n)$ to $(x_{\sigma(1)} \cdots x_{\sigma(n)})$.*

Two equivalent codes have the same capability of correcting errors, so we can study linear codes up to this equivalence. It is clear from linear algebra that every code is equivalent to a code with its matrix in canonical form. If G is a generator matrix in canonical form, the first k symbols of a words are called **information symbols**, while the remaining ones are the **control symbols**. Given an $[n, k]$-code C, we define the **dual code** of C as the vector space

$$C^\perp = \{y \in \mathbb{F}_q^n \mid y \circ x = 0 \ \forall x \in C\}.$$

$C^\perp$ is a $[n, n-k]$-code. Remark that if $C^\perp$ has generator matrix H, then $x \in C$ if and only if $xH^\top = 0$. H is said to be a **control matrix** for C and, if C has a generator matrix $G = \begin{pmatrix} I_k & P \end{pmatrix}$ then $H = \begin{pmatrix} -P^\top & I_{n-k} \end{pmatrix}$. If $C = C^\perp$ then we say that C is self-dual.

We introduce now one of the easiest decoding methods for linear codes, called **syndrome methods**. Let C be a $[n, k]$-code with control matrix H. The syndrome of $x \in \mathbb{F}_q^n$ is the vector $xH^\top \in \mathbb{F}_q^{n-k}$. We saw that the code words are those with syndrome equal to 0. Recalling that C is a subgroup of $\mathbb{F}_q^n$, we can divide $\mathbb{F}_q^n$ in cosets of C. The elements of the same coset are identified by the same syndrome. Now suppose we received $y = x + v \in \mathbb{F}_q^n$, where x is the sent code word and v the error vector; y and v have the same syndrome, so, in order to decode in accord with the maximum-likelihood-decoding principle, we choose a vector with minimum weight among those with the same syndrome of y. For every coset, the chosen vector is called the **coset leader**. The decoding is therefore reduced to the calculation of a syndrome and the comparison with the q^{n-k} possible syndomes, previously calculated and associated to a coset leader. This method is fast when q^{n-k} is small compared to n, i.e. when the information rate k/n is close to 1. If a code has minimum distance $d = 2e + 1$, then every vector of weight less or equal e is the unique coset leader of a coset, since two vector of weight less or equal e have distance at most $2e$, so they belong to different cosets. Moreover, if the code is perfect, there are no further coset leaders.

2 Algebraic geometric codes on curves

2.1 AG codes

Let X be a smooth projective curve of genus g over $\mathbb{F}_q$. Indicate with $\mathbb{F}_q(X)$ the set of rational functions over $\mathbb{F}_q$ and with $Div(X)$ the set of divisors of X. In $Div(V)$ define the equivalence relation $\approx$. $D \approx D'$ (D is linearly equivalent to D') : $\iff$ $D - D' = (f)$ for any $f \in \mathbb{F}_q(X)$, i.e. if and only if they differ for a principal divisor. The group $Div(X)/\approx$ is called the **Picard group** and indicated with $Pic(X)$. In the following, writing $D \succeq D'$, we will mean that the divisor $D - D'$ is effective. For a divisor let $D \in Div(X)$, $L(D) := \{f \in \mathbb{F}_q(X)^* \mid (f) + D \succeq 0\} \cup \{0\}$.

Definition 2.1 *Let $G \in Div(X)$, $\{P_1, \cdots, P_n\}$ be rational points over $\mathbb{F}_q$ with $\{P_1, \cdots, P_n\} \cap \operatorname{supp}(G) = \emptyset$, and put $D := P_1 + \cdots + P_n \in Div(X)$. The **algebraic geometric code** (or, for short, AG codes) $C(X, D, G)$ is the image of the linear map*

$$\alpha : L(G) \longrightarrow {\mathbb{F}_q}^n$$
$$f \longmapsto (f(P_1), \cdots, f(P_n)).$$

Proposition 2.1 *Let X, D and G be as above, k and d respectively the dimension and the minimum distance of the code $C(X, D, G)$. Hence*

1. *$k = dimL(G) - dimL(G - D)$. In particular, if $n > \deg G$, then $k = dimL(G)$. Moreover, if $2g - 2 < \deg G$, then $k = \deg G + 1 - g$.*
2. *$d \geq n - \deg(G)$.*

Proof:

1. Let $f \in \ker \alpha$. Therefore f vanishes in $P_1, \cdots, P_n$. Since $P_1, \cdots, P_n \notin \operatorname{supp}(G)$, $f \in L(G - D)$. If $n > \deg G$, $L(G - D) = \{0\}$; hence α is injective and $k = \dim L(G)$. Moreover, if $2g - 2 < \deg G$, $k = \deg G + 1 - g$ by the Riemann-Roch theorem.
2. If d is the minimum distance of the code, there exists $f \in L(G)$ such that $\alpha(f)$ has weight $d > 0$. Assume $f(P_i) \neq 0$ for $i = 1, \cdots, d$, and $f(P_i) = 0$ for $i = d + 1, \cdots, n$. Thus $f \in L(G - P_{d+1} - \cdots - P_n)$. As $f \neq 0$, $\deg G - (n - d) = \deg(G - P_{d+1} - \cdots - P_n) \geq 0$, so $d \geq n - \deg G$. □

REMARK: If we discard the hypothesis $\operatorname{supp}(G) \cap \operatorname{supp}(D) = \emptyset$, we can still associate a code $C(X, D, G)$ to (X, D, G) by choosing $t \in \mathbb{F}_q(X)$ with $ord_{P_i}(t) =$ multiplicity of P_i in G and sending $f \in L(G - (t))$ to the n-uple $(f(P_1), \cdots, f(P_n))$. The previous proposition still holds, but the choice of t is not unique and choosing a different t with the same properties we get a different code. We will define soon an equivalence relation between codes such that different choices for t will produce equivalent codes.

2.2 Dual AG codes

In this section we will define the code $C^*(X, D, G)$, called the dual algebraic geometric code associated to (X, D, G). Indicate with $\Omega(X)$ the set of rational differential form on X and, for $E \in Div(X)$, let $\Omega(E) = \{\omega \in \Omega(X)^* \mid (\omega) - E \succeq 0\}$. In the following let W be a canonical divisor for X, $W = \omega$ with $\omega \in \Omega(X)$. Clearly, if we choose a different rational differential form ω', $\omega' = f\omega$ for any $f \in \mathbb{F}_q(X)$, hence $(w') \approx W$.

Definition 2.2 *The **dual algebraic geometric code** $C^*(X, D, G)$ is the image of the linear map*

$$\alpha^* : \Omega(G - D) \longrightarrow {\mathbb{F}_q}^n$$

$$\eta \longmapsto (res_{P_1}(\eta), \cdots, res_{P_n}(\eta)),$$

where $res_{P_i}(\eta)$ is the residue of η at the point P_i.

REMARK: It is easy to verify that, if $E \in Div(X)$, the application from $L(W - E)$ to $\Omega(E)$ which sends f to $f\omega$ is a bijection. Therefore, equivalently, $C^*(X, D, G)$ is the image of

$$\beta^* : L(W + D - G) \longrightarrow {\mathbb{F}_q}^n$$

$$f \longmapsto (res_{P_1}(f\eta), \cdots, res_{P_n}(f\eta))$$

Proposition 2.2 *Let X, D and G as above, and let k^* and d^* be respectively the dimension and the minimum distance of the code $C^*(X, D, G)$.*

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

Proof:

1. The kernel of β^* is $L(W - G)$. If $\deg G > 2g - 2$ then β^* is injective. Last statement follows from the Riemann-Roch theorem.
2. Analogously to what we did in Proposition 2.1, consider a code word of weight d^* and observe that, up to re-enumeration of $P_1, \cdots, P_n$, it is equal to $\alpha^*(\eta)$ for some non-zero η in $\Omega(G - P_1 - \cdots - P_d)$. Therefore $\dim \Omega(G - P_1 - \cdots - P_d) = \dim L(W - G + P_1 + \cdots P_n) \geq 1$ and we conclude that the degree of such divisor is greater or equal 0. □

From what we said so far, it is clear that, in order to calculate more easily the parameters of the code and have a positive distance, it is better to choose divisors D and G such that $2g - 2 < \deg G < \deg D$.

Theorem 2.1 *The codes $C(X, D, G)$ and $C^*(X, D, G)$ are dual to each other.*

Proof: First we show that $C^*(X, D, G) \subseteq C(X, D, G)^\perp$. Let $\eta \in \Omega(G - D)$, $f \in L(G)$. We have to show that $\alpha(f) \circ \alpha^*(\eta) = 0$. But $\alpha(f) \circ \alpha^*(\eta) = \sum_{i=1}^n f(P_i) res_{P_i}(\eta)$. Remark that the rational differential form $f\eta$ belongs to $\Omega(-D)$, it can have simple poles just in the support of D. Hence $\sum_{P \in X} res(f\eta) = \sum_{i=1}^n res_{P_i}(f\eta) = \sum_{i=1}^n f(P_i) res_{P_i}(\eta)$. We conclude, by the residues theorem, that $\alpha(f) \circ \alpha^*(\eta) = 0$. Furthermore we know that

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

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

Thus $C^*(X, D, G) = C(X, D, G)^\perp$. □

The following theorem shows that every dual algebraic geometric codes can be obtained as algebraic geometric code and viceversa.

Lemma 2.1 *There exists a differential form ω with simple poles with residues 1 in the points of the support of D and such that $C(X, D, W + D - G) = C^*(X, D, G)$, where $W = (\omega)$.*

Proof: Chosen $\eta \in \Omega(X)$, let $f \in \mathbb{F}_q(X)$ be such that $ord_{P_i} f = -(ord_{P_i} \eta + 1)$. The function $f\eta$ has simple poles in $P_1, \cdots, P_n$. We can multiply $f\eta$ with a rational function to obtain residues equal to 1 in those simple poles. Let ω have such properties and let $W = (\omega)$. For every $f \in L(W + D - G)$ we have $res_{P_i}(f\omega) = f(P_i) res_{P_i}(\omega) = f(P_i)$. Then $\alpha(f) = \beta^*(f)$ and so we finally get $C(X, D, W + D - G) = C^*(X, D, G)$. □

We saw in section 1 that two codes are called equivalent if they differ for a fixed permutation of the coordinates. We introduce a new equivalence relation between codes such that it reflects, in some sense, the equivalence relation between divisors. From now, when we will talk about equivalent codes, we will mean equivalent according to the following definition.

Definition 2.3 *Two codes C_1 and C_2, of length n over $\mathbb{F}_q$, are called equivalent if there exists $\gamma \in (\mathbb{F}_q^*)^n$ such that $\gamma C_1 = C_2$.*

REMARK: It is clear that the dimension and the distribution of weights of a code are not changed by the multiplication with a non zero element $\gamma \in (\mathbb{F}_q^*)^n$. We will study the properties of a code up to equivalence. It will be useful also to decode a given encoded message.

Lemma 2.2 *Let $D = \sum_{i=1}^n P_i$ be as above, $G, G' \in Div(X)$ whose supports are disjoint sets from the ones of D and D', $G \approx G'$. Then $C(X, D, G)$ is equivalent to $C(X, D, G')$ and $C^*(X, D, G)$ is equivalent to $C^*(X, D, G')$.*

Proof: Let $(g) = G - G'$ for $g \in \mathbb{F}_q(X)$. Since the supports of G and G' are disjoint from $supp(D)$, $g(P_i) \neq 0$, the multiplication with g is an isomorphism between $L(G)$ and $L(G')$ and between $\Omega(G-D)$ and $\Omega(G'-D)$. Therefore $C(X, D, G) = \gamma C(X, D, G')$ and $C^*(X, D, G) = \gamma C^*(X, D, G')$, where $\gamma = (g(P_1), \cdots, g(P_n))$. □

Proposition 2.3 *Let $G \in Div(X)$ be such that $2G \approx W + D$. Then $C(X, D, G)$ is equivalent to its dual code.*

Proof: It follows directly from Proposition 2.1 and Lemmas 2.1 and 2.2. □

REMARK: The viceversa in Proposition 2.3 does not hold. A counterexample can be found in [4, Remark 1 p. 894].

The next theorem gives an equivalent condition for the existence of G such that $2G \approx W + D$.

Theorem 2.2 (Weil) *There exists G such that $2G \approx W + D$ if and only if D is a square in $Pic(X)$.*

From what we saw previously it is quite natural to state the following lemma, which gives a sufficient condition to be self-dual.

Lemma 2.3 *If there exists $\eta \in \Omega(X)$ with simple poles and residues equal to 1 in the poles of the support of D and such that $2G = K + D$ for $K = (\eta)$, then $C(X, D, G)$ is self-dual*

Proof: Let ω and W be as in Lemma 2.1. We have $\eta = f\omega$ for some non zero rational function f. Thus $K + D - G \approx W + D - G$ and, by the proof of the previous lemma, $C(X, D, K + D - G) = \gamma C(X, D, W + D - G)$ where $\gamma = (f(P_1), \cdots, f(P_n))$. But $f(P_i) = res_{P_i}\eta / res_{P_i}\omega = 1$, so $C(X, D, G) = C(X, D, K + D - G) = C(X, D, W + D - G) = C^*(X, D, G) = C(X, D, G)^{\perp}$. □

In general this condition is just a sufficient one. It is proved in [18, 3.12] that, if $n > 2g + 2$, then the condition is also a necessary one.

Let us now investigate the relations between the parameters of algebraic geometric codes.

Lemma 2.4 *Let $2g - 2 < \deg G < n$, 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 lower bounds are the ones proved in Lemmas 2.1 and 2.2, while the upper ones are the singleton bounds. □

Corollary 2.1 *Let $2g-2 < \deg G < n$. If $g = 0$ then the codes $C(X, D, G)$ and $C^*(X, D, G)$ are MDS.*

We saw some bounds for the distance of algebraic geometric codes. We would like now to see the distance as a geometric property of the divisors D and G. Following what we did in the proof of Proposition 2.1, we remark that $x \in C(X, D, G)$ has weight $r > 0$ if $x = \alpha(f)$, with f different from 0 at r points among $\{P_1, \cdots, P_n\}$ and vanishing at $n - r$ points. Thus $f \in L(G - P_{i(r+1)} - \cdots - P_{i(n)})$ for some $i \in S_n$. It follows that there exists a divisor $D' \preceq D$ of degree $n-r$ such that $L(G - D') \neq \{0\}$. In our case we can assume that α is injective, i.e. $\deg G < n$. If there exists $D' \preceq D$ with $\deg D' = n-d$ then there exists a non zero word of weight $\leq d$ in $C(X, D, G)$. So we have that the minimum distance of $C(X, D, G)$ is the smallest integer d such that there exists a divisor $D' \preceq D$ with $L(G - D') \neq \{0\}$. Hence the minimum distance of a code can be obtained by looking at some subspaces of $L(G)$.

Analogously, if $\deg G > 2g - 2$, the minimum distance of $C^*(X, D, G)$ is the smallest integer d^* such that there exists a divisor $D' \preceq D$ of degree d with $L(W + D' - G) \neq \{0\}$. We can state this sentence in the following way: $x \in C^*(X, D, G)$ has weight $r > 0$ if $x = \beta^*(f)$ for some $f \in L(W + D - G)$ such that $f\omega$ has non zero residue at r points among $\{P_1, \cdots, P_n\}$ and zero residue in the remaining ones. Then $f\omega$ is regular at $n - r$ points and $(f\omega) + \sum_{j=1}^{r} P_{i(j)} + G = E$, where E is an effective divisor with support disjoint from $\{P_{i(1)}, \cdots, P_{i(r)}\}$. So $G - W \approx -\sum_{j=1}^{r} P_{i(j)} + E$. Viceversa, if the last equality holds, then $C^*(X, D, G)$ has a word of weight r. This allows us to state the following theorem.

Theorem 2.3 *The minimum distance d^* of $C^*(X, D, G)$ is the smallest number of distinct points $P_{i(1)}, \cdots, P_{i(d^*)}$ in the support of D such that, in $Pic(X)$, $G - W = \sum_{j=1}^{d^*} P_{i(j)} - E$ for any effective divisor E with support disjoint from $P_{i(1)}, \cdots, P_{i(d^*)}$.*

Arguing this way we can compute the distribution of weights; in fact the number of code words with weight r is equal to $(q - 1)$ times the number of divisors $D' \preceq D$ of degree r linearly equivalent to a divisor of the form $G - W + E$ for some $E \in L(0)$, $\operatorname{supp} D' \cap \operatorname{supp} E = \emptyset$.

2.3 Rational points on curves and lower bounds

Let us deal again with the parameters of the algebraic geometric codes. We know that one of the central problems of coding theory is finding codes with relative distance δ and rate R as large as possible. Let V_q be the set of pairs

(δ, R) coming from a linear code over $\mathbb{F}_q$ and U_q the set of limit points of V_q. Manin proved the following theorem, that gives us some information about U_q.

Theorem 2.4 *There exists a function $\alpha : [0,1] \to [0,1]$ such that $U_q = \{(\delta, R) \mid 0 \leq R \leq \alpha(\delta)\}$. α is continuous in $[0, \frac{q-1}{q}]$, vanishes in $[\frac{q-1}{q}, 0]$ and is strictly decreasing.*

Proof: see [17, th. 8 p. 2614]

REMARK: The function α above is exactly the same α we defined in section 1. We already know, by the Gilbert bound, that $1 - H_q(\delta) \leq \alpha(\delta)$.

For an algebraic geometric code $C(X, D, G)$, we deduce by Proposition 2.1, if $\deg G < n$, that

$$\delta + R \geq \frac{n - \deg G}{n} + \frac{\deg G + 1 - g + \dim L(W - G)}{n} \geq 1 + \frac{1-g}{n}.$$

So we would like to find a family of codes with n going to infinity and g/n as small as possible asymptotically.

Lemma 2.5 *Let $\{X_i \mid i \in \mathbb{N}\}$ be a sequence of smooth projective curves over $\mathbb{F}_q$, $g_i := g(X_i)$ and $N_1(X_i)$ the number of rational points (of degree 1) of X_i. If g_i tends to infinity and $\lim_{i \to +\infty} \frac{g_i}{N_1(X_i)} = \gamma$, then the intersection of the line $\delta + R = 1 - \gamma$ with the square $[0,1] \times [0,1]$ is contained in U_q.*

Proof: Let (δ, R) be a point of the line intersected with the square. Since γ is not negative, we have $\delta = 1$ iff $\gamma = 0$ and it is clear that $(1,0) \in U_q$. We can restrict to $\delta < 1$. Consider the codes $C_i := C(X_i, D_i, G_i)$, where D_i is the sum of all the rational points $P_1, \cdots, P_{N_1(X_i)}$ of X_i and $G_i := \lfloor N_1(X_i)(1-\delta) \rfloor P_1$. The supports of D_i and G_i are not disjoint, but this is not a problem, as shown by the remark of page 11. R_i tends to $\bar{R} = R + l \geq R$, where $l := \lim_{i \to +\infty} \frac{\dim L(W_i - G_i)}{n_i}$. Let $\bar{\delta} = \lim_{i \to +\infty} \delta_i$. Now, we know that $\delta_i + R_i \geq 1 + \frac{1 - g_i + \dim L(G_i - W_i)}{n_i}$, so $\bar{\delta} + \bar{R} \geq 1 - \gamma + l$. Therefore $\bar{\delta} \geq 1 - \gamma - \bar{R} + l = 1 - \gamma - R = \delta$. Therefore the point $(\bar{\delta}, \bar{R})$ is in U_q and $\bar{R} \geq R$, $\bar{\delta} \geq \delta$. By the previous theorem, $(\delta, R) \in U_q$. □

NOTE: In the proof of [24][Part II, 5.2] the author discards l and says that R_i tends to $1 - \delta - \gamma = R$. We are not sure this is true in general. In any case, as we showed in the proof, it is sufficient to prove that R_i tends to a value greater or equal R.

Corollary 2.2 *Assuming the same hypotheses of the previous lemma, we have $\alpha(\delta) \geq 1 - \delta - \gamma$.*

Let $N_q(g) := \max\{\#X(\mathbb{F}_q) \mid X \text{ is a smooth projective curve of genus } g \text{ over } \mathbb{F}_q\}$. It is clear by what we said above that we would like to know the value of $N_q(g)$ and the function

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

To this end, we define the zeta function associated to a curve over $\mathbb{F}_q$ and later on we will show how it is related to the number of rational points. Let $s \in \mathbb{C}$, X a smooth projective curve over $\mathbb{F}q$.

$$\zeta(X,s) := \prod_p (1 - N(p)^{-s})^{-1},$$

where the product is over all the closed points of X and $N(p) = q^{\deg p}$. Equivalently,

$$\zeta(X,s) = \sum_{D\succeq 0} N(D)^{-s},$$

where the sum runs over all the effective divisors of X and $N(D) = q^{\deg D}$. Let δ be the g.c.d. of all the degrees of the effective divisors on X.

REMARK 1: The integer δ divides $2g-2$. In fact, by the Reimann-Roch theorem, $\dim L(W) > 0$ and so there exists an effective divisor of degree $2g-2$.

REMARK 2: If $n > 2g-2$ and $n = k\delta$, then there exists an effective divisor of degree n. Indeed we can write δ as a linear combination of degrees d_i coming from effective divisors D_i. $\delta = \sum_{i=1}^m a_i d_i$ where $a_i \in \mathbb{Z}$. Therefore $D := k\sum_{i=1}^m a_i D_i$ has degree n. Recalling $\dim L(D) = \deg D + 1 - g > 0$ and choosing $f \in L(D) \setminus \{0\}$, we obtain that $(f) + D$ is the wanted divisor.

For $m \in \mathbb{Z}$, let $Pic_m(X) = \{[D] \in Pic(X) \mid \deg D = m\}$. This is clearly a good definition, because principal divisors have degree 0. If there exists a divisor D' of degree m, then $\#Pic_m(X) = \#Pic_0(X) := h$ via the bijection $[D] \mapsto [D] - [D']$.

Lemma 2.6 *The number a_n of effective divisors of degree n is equal to*

$$\sum_{[D]\in Pic_n(X)} \frac{q^{\dim L(D)} - 1}{q-1}.$$

Proof: If $[D] \in Pic_n(X)$ then $D + (f)$ is an effective divisor of degree n for every $f \in L(D) \setminus \{0\}$. Moreover $[D] + (f) = [D'] + (f')$ implies $[D] = [D']$ and $f/f' \in \mathbb{F}_q^*$. □

We immediately deduce the following theorem from Riemann-Roch's theorem and what we observed previously:

Corollary 2.3 *If $n > 2g-2$ then $a_n = h\frac{q^{n+1-g}-1}{q-1}$.*

Changing variables, we can write $\zeta(X,s) = Z(X,q^{-s}) = Z(X,t)$ for $s,t \in \mathbb{C}$; so we have a power series that converges for $|t| < 1$. The zeta function becomes

$$\zeta(X,s) = \sum_{n\geq 0} a_n q^{-sn} = \sum_{n=0}^{2g-2} a_n t^n + \sum_{n=2g-1}^{+\infty} a_n t^n,$$

where the index n in the second sum runs over the multiples of δ bigger than $2g-2$. By REMARK 1 at page 17, if we put $e = (2g-2+\delta)/\delta$, $e\delta$ is the smallest multiple of δ larger than $2g-2$. Hence we have

$$Z(X,t) = \sum_{n=0}^{2g-2} a_n t^n + \sum_{n=e}^{+\infty} a_{n\delta} t^{n\delta} =$$

$$polynomial + \frac{h}{q-1}\sum_{n=e}^{+\infty}(q^{n\delta+1-g}-1)t^{n\delta}$$

$$= \frac{h}{q-1}\left(\frac{q^{g+1+\delta}t^{2g-2+\delta}}{1-(qt)^\delta} - \frac{t^{2g-2+\delta}}{1-t^\delta}\right).$$

This way we obtained a rational function of t with poles at $t^\delta = 1$ and $(qt)^\delta = 1$.

The following theorems are the fundamental connection between the zeta function and our problem.

Theorem 2.5

$$Z(X,t) = \frac{P_1(t)}{P_0(t)P_2(t)}$$

where $P_0 = 1-t$, $P_2 = 1-qt$, $P_1 = \prod_{i=1}^{g}(1-\alpha_i t)(1-\bar{\alpha_i})$ and α_i are algebraic integers of absolute value $q^{\frac{1}{2}}$.

Proof: The proof in [2] uses only Riemann-Roch's theorem, while the original one, due to Weil, needs intersection theory.

Let us indicate with N_r the number of points of degree one over $\mathbb{F}_{q^r}$

Theorem 2.6 (Hasse-Weil bound) $|N_r - (1+q^r)| \leq 2g\sqrt{q^r}$.

A curve with exactly $1 + q + 2g\sqrt{q}$ points over $\mathbb{F}_q$ is called **maximal**. We said that an equivalent expression for ζ is

$$\zeta(X, s) = \prod_p (1 - N(p)^{-s})^{-1} = \prod_{r \geq 1} (1 - q^{-sr})^{-N_r}$$

Expanding the log of the zeta function in its Taylor series, we have

$$\log Z(X, t) = \sum_{r \geq 1} -N_r \log(1 - t^r) = \sum_{r \geq 1} \frac{N_r}{r} t^r$$

Hence, by Theorem 2.5,

$$\log Z(X, t) = \log P_1(t) - \log P_0(t) - \log P_2(t) =$$

$$= \sum_{i=1}^{g} (\log(1 - \alpha_i t) + \log(1 - \bar{\alpha_i} t)) - \log(1 - t) - \log(1 - qt) =$$

$$\sum_{r=1}^{+\infty} \frac{1 + q^r - \sum_{i=1}^{g} (\alpha_i + \bar{\alpha_i}^r)}{r} t^r$$

This means that the knowledge of the α_i's is enough to compute N_r for every r. For $r = 1$ we have $N_1 = 1+q+a_1$ and $|a_1| = 2g\sqrt{q}$, so $N_1 \leq 1+q+2g\sqrt{q}$. We can now go back to the problem of finding the value (or at least some bounds) for $A(q)$. It is clear that $N_q(g) \leq 1 + q + 2g\sqrt{q}$, so

$$A(q) = \lim_{g \to \infty} \frac{N_q(g)}{g} \leq 2\sqrt{q}.$$

The first improvement of this bound is due to Ihara ([10, p. 721]).

Theorem 2.7 *For every q we have $A(q) \leq \frac{\sqrt{8q+1}-1}{2}$.*

Proof: Let $b_i = \alpha_i + \bar{\alpha_i} \in \mathbb{R}$. We have

$$q + 1 - \sum_{i=1}^{g} b_i = N_1 \leq N_2 = q^2 + 1 - \sum_{i=1}^{g} (\alpha_i^2 + \bar{\alpha_i}^2) = q^2 + 1 + 2gq - \sum_{i=1}^{g} b_i^2$$

By the Cauchy's inequality we get

$$g \sum_{i=1}^{g} b_i^2 \geq (\sum_{i=1}^{g} b_i)^2,$$

hence

$$N_1 \leq q^2 + 1 + 2gq - g^{-1} (\sum_{i=1}^{g} b_i)^2 = q^2 + 1 + 2gq - g^{-1} (N_1 - 1 - q)^2.$$

We get a quadratic equation on N_1:

$$N_1^2 - (2q + 2 - g)N_1 + (q + 1)^2 - (q^2 + 1)g - 2qg^2 \leq 0.$$

It turns out that

$$N_1 \leq \frac{2q + 2 - g + \sqrt{(8q + 1)g^2 + (4q^2 - 4q)g}}{2}$$

and so

$$A(q) \leq \lim_{g \to +\infty} \frac{2q + 2 - g + \sqrt{(8q + 1)g^2 + (4q^2 - 4q)g}}{2g} = \frac{\sqrt{8q + 1} - 1}{2}.$$

□

Arguing analogously, Drienfeld and Vladut ([26, th. 1]) proved that, for every prime power q, we have $A(q) \leq \sqrt{q} - 1$. On the other hand, the following theorem proves that we have an equality for the even powers of a prime number.

Theorem 2.8 (Tsfasman, Vladut, Zink) *Let $q = p^{2m}$ be an even power of the prime p. Then there is a sequence of curves X_i, defined over $\mathbb{F}_q$ having genus g_i and N_i rational points, such that*

$$\lim_{i \to \infty} \frac{N_i}{g_i} = \sqrt{q} - 1.$$

Proof: see [22, p. 28]

Using Lemma 2.5 we can state the following corollary:

Corollary 2.4 *If $q = p^{2m}$ is an even power of a prime, then $\alpha(\delta) \geq 1 - \delta - (\sqrt{q} - 1)^{-1}$.*

It easy to check that the line $R = 1 - \delta - (\sqrt{q} - 1)^{-1}$ intersects the Gilbert curve $R = 1 - H_q(g)$ for $q \geq 43$ and, since q has to be a square, we have an improvement of Gilbert bound for $q \geq 49$.

3 Decoding methods

A code is useful only if there exists an efficient way of decoding. Let us introduce now two algorithms for decoding dual geometric codes. The first one has been discovered by Skorobogatov and Vladut in 1990 and will be called SV-algorithm for short. Nevertheless it is the easiest one and it is not able to decode the full capability of the codes. Indeed we know that if d is the minimum distance of a code, a good algorithm should be able to correct every error of weight at most t, where $2t < d$. We will see that the SV-algorithm can surely correct errors of weight t if $2t < d - g$, where g is, as usual, the genus of the curve X but it could not work for larger values of t. This is a non trivial restriction, since we saw that good codes are based on curve with high genus. In order to solve this problem, Duursma improved in 1992 the SV-algorithm and produced the more efficient processor we will describe later. The main idea of Duursma algorithm is to use a majority voting scheme. This technique has been used for the first time by Feng and Rao to extend the first decoding algorithm for geometric codes, published by Justesen in 1989.

3.1 SV-algorithm

Let $C^*(X, D, G)$ be a fixed dual geometric code based on a curve X of genus g, $D = P_1 +, \cdots, +P_n$ and $2g-2 < \deg G$. The designed distance of the code is $\deg G - (2g - 2)$. Suppose we transmit a word c and the vector $f = c + e$ is received.

Definition 3.1 *For any vector $f \in \mathbf{F}_q{}^n$ and any function φ in the function field, the syndrome of f with respect to f is denoted by $\varphi \circ f$ and defined by $\varphi \circ f = \sum_{i=1}^{n} \varphi_i(P_i) f_i$. By convention we put $\varphi \circ f = \infty$ if φ has a pole in any P_i.*

The dual of $C^*(X, D, G)$ is the code $C(X, D, G)$, so c belongs to $C^*(X, D, G)$ if and only if $x \circ c = 0$ $\forall x \in C(X, D, G)$, hence if and only if $\varphi \circ c = 0$ $\forall \varphi \in L(G)$. It means that c is a word of the code if and only if, chosen a basis $\{\varphi_1, \cdots, \varphi_u\}$ of $L(G)$, the syndromes of c with respect to φ_i is 0 for $i = 1, \cdots, u$. Moreover, for every $\varphi \in L(G)$, $\varphi \circ e = \varphi \circ f$. What we try to do in the following is to deduce the error vector e from the syndromes of f.

Definition 3.2 *An **error location** for e is a point P_i such that $e_i \neq 0$. An **error locator** for e is a function Θ with no poles among $P_1, \cdots, P_n$ and such that $\Theta(P_i) = 0$ for every error location P_i.*

Proposition 3.1 *Let e have weight at most t and A be a divisor with no poles among $P_1, \cdots, P_n$ such that $\dim L(A) \geq t + 1$. Then an error locator in $L(A)$ exists.*

Proof: Let M be the support of e, i.e. the set of points P_i such that $e_i \neq 0$. A function Θ is an error locator for e if and only if $\Theta(P_i) = 0 \; \forall P_i \in M$. Let now $\{\varphi_1, \cdots, \varphi_s\}$ be a basis of $L(A)$. A linear combination $a_1\varphi_1 + \cdots + a_s\varphi_s$ is an error locator if and only if

$$a_1\varphi_1(P_i) + \cdots + a_s\varphi_s(P_i) = 0 \; \forall \, P_i \in M.$$

This is a system of at most t equations in s unknowns and, by hypothesis, $s > t$, so it has a non-trivial solution. □

The next proposition shows why finding an error locator is so important for our purpose.

Proposition 3.2 *Let e be an error vector of weight at most t, A and Z two divisors on X with support disjoint from $\{P_1, \cdots, P_n\}$, such that $\deg A \leq t + r$ and $\deg Z \geq t + r + 2g - 1$ for some $r \geq 0$. If there exists an error locator Θ in $L(A)$ then e is uniquely determined by Θ and the syndromes of e with respect to the functions in $L(Z)$.*

Proof: Let M' be the set of points where Θ vanishes. Clearly M' contains M, the support of e. M' has at most $t + r$ points. It is clear that $\varphi \circ e = \sum_{P_i \in M'} \varphi(P_i)e_i$ for every function without poles among $P_1, \cdots, P_n$. This is true, in particular, for every function $\varphi \in L(Z)$, so e is a solution of the equation

$$\varphi \circ x = \sum_{P_i \in M'} \varphi(P_i)x_i \quad \forall \, \varphi \in L(Z).$$

If e' is another solution, then $\varphi \circ (e - e') = 0 \forall \varphi \in L(Z)$. It means that $e - e'$ belongs to $C^*(X, D, Z)$. The minimum distance of this code is not less than $t + r + 1$ but if e and e' have both support in M' then $e - e'$ has weight at most $t + r$. Therefore $e = e'$. □

REMARK: We are trying to decode f, so we do not know e. In particular, we do not know how to find an error locator for e and how to calculate the syndromes. The second problem can be solved by choosing $Z \preceq G$. In this case the syndromes can be calculated from f instead of e. The solution of the second problem is treated in the next proposition and it requires the the introduction of a further auxiliary divisor.

Proposition 3.3 *Let e have weight at most t and Y be a divisor with support disjoint from the support of D such that $\deg Y \geq t + 2g - 1$. Then a function Θ without poles among $P_1, \cdots, P_n$ is an error locator for e if and only if $\Theta\chi \circ e = 0$ for every $\chi \in L(Y)$.*

Proof: Let $e' = (\Theta(P_1)e_1, \cdots, \Theta(P_n)e_n)$. So we have $\Theta\chi \circ e = \sum_{i=1}^{n} \theta(P_i)\chi(P_i)e_i = \chi \circ e'$. We will have that Θ is an error locator if and only if $e' = 0$. So, if

Θ is an error locator then $\Theta\chi \circ e = 0$ for every function. Viceversa, suppose $\chi \circ e' = 0$ for every $\chi \in L(Y)$. It means that $e' \in C^*(X, D, Y)$. Recalling that $\deg Y \geq t + 2g - 1$, we get that the distance of this code is greater than t. This implies $e' = 0$. □

Corollary 3.1 *Let $S = (\psi_i \chi_j)_{i,j}$, where the elements ψ_i form a basis of $L(A)$ and the $\chi_j' s$ are a basis of $L(Y)$. Then $\Theta = \sum_i a_i \psi_i$ is an error locator for e in $L(A)$ if and only if $\sum_i a_i S^i = 0$, where S^i is the ith row of S.*

REMARK: Again, we want to calculate the syndromes of e from those of f. If $Y + A \preceq G$ then $\Theta\chi \in L(G)$ for every $\Theta \in L(A)$ and $\chi \in L(Y)$, so this is allowed.

Summarizing, we are looking for three auxiliary divisors A, Z and Y with the required properties. Assume that $\deg G > 2g - 2$.

Lemma 3.1 *Suppose there exists a divisor A' such that $\deg A' \leq \deg G - (2g-1) - t$ and $\dim L(A') \geq t+1$. Then there exist A, Z and Y with $Z \preceq G$, $Y + A \preceq G$ and satisfying the hypotheses of the previous propositions.*

Proof: If the support of A' is disjoint from $\{P_1, \cdots, P_n\}$, set $A = A'$, otherwise add a suitable principal divisor. The first condition implies that, for some $u \geq 0$, $t + 1 + u = \dim L(A) \geq \deg A + 1 - g$, so $\deg A \leq t + u + g$ and $\deg A = t + r$ for some $r \geq 0$. We can now put $Z = G$ and $Y = G - A$. We get $\deg Z = \deg G \geq A + (2g - 1) + t \geq r + t + 2g - 1$ and $\deg Y \geq \deg G - \deg G + 2g - 1 + t = t + 2g + 1$. □

The conditions of Lemma 3.1 guarantees that $2t < d$, so the code can correct errors of weight t. We wondering when there exists a divisor A' such that $\deg A' \leq \deg G - (2g-1) - t$ and $\dim L(A') \geq t+1$. We give now a sufficient condition.

Lemma 3.2 *If $2t < \deg G - (3g - 2)$, then A' with the required properties exists.*

Proof: By the hypothesis, $t + g \leq \deg G - 2g + 1 - t$, so there exists a, with $t + g \leq a \leq \deg G - 2g + 1 - t$. Set $A' = aQ$, where Q is a point not in the support of D. $\dim L(A') \geq t + g + 1 - g = t + 1$. □

It is clear now what our strategy to decode a message is. Let us write formally the SV-algorithm.

SV-ALGORITHM: Let c be a word of the code $C^*(X, D, G)$ defined over a

curve of genus g, with $\deg G > 2g-2$. Let $f = c + e$, where e is the error vector.

STEP 0: Preliminary step
This step is performed only once for any code. Choose a divisor A such that $\dim L(A) > t$ and $\deg A \leq \deg G - (2g-1) - t$. Choose divisors Z, Y such that $Z \preceq G, Y + A \preceq G$, $\deg Z \geq \deg A + 2g - 1$ and $\deg Y \geq t + 2g - 1$. Choose bases $\{\varphi_1, \cdots, \varphi_u\}$ of $L(Z)$, $\{\psi_1, \cdots, \psi_s\}$ of $L(A)$ and $\{\chi_1, \cdots, \chi_r\}$ of $L(Y)$.

STEP 1: Syndrome calculation
Calculate the matrix $S = (\psi_i \chi_j \circ f)_{i,j}$.

STEP 2: Error locator
Find $\alpha_1, \cdots, \alpha_s$ such that $\alpha_1 S^1 + \cdots + \alpha_s S^s = 0$, where S^i is the ith row of S. $\Theta = \sum_{i=1}^{s} \alpha_i \psi_i$ is an error locator for e in $L(A)$.

STEP 3: Error locations
Let M' be the set of points where Θ vanishes. This set contains the error locations.

STEP 4: Error values calculation
Solve the system of equations

$$\sum_{P_l \in M'} \varphi_i(P_l) e_l = \varphi_i \circ f \qquad \text{for } i = 1, \cdots, u.$$

Extend the solution by putting $e_j = 0$ if $P_j \notin M'$. $(e_1, \cdots, e_n)$ is the error vector.

3.2 A cubic curve

Before introducing the Duursma algorithm, we will give an example of geometric code and we will use the SV-algorithm to correct en error of weight 2 produced during the transmission of a word. The curve X is given by the equation $x^3 + y^3 + z^3 = 0$.

- **Points over $\mathbb{F}_2$**

  $P_0 = (0:1:1) \qquad P_1 = (1:1:0) \qquad P_2 = (1:0:1)$

- **Points over $\mathbb{F}_4 = \frac{\mathbb{F}_2[z]}{(x^2+x+1)} = \mathbb{F}_2[\alpha]$**

points over $\mathbb{F}_2$
$P_3 = (\alpha : 1 : 0)$ $P_4 = (\alpha + 1 : 1 : 0)$ $P_5 = (\alpha : 0 : 1)$
$P_6 = (\alpha + 1 : 0 : 1)$ $P_7 = (0 : \alpha : 1)$ $P_8 = (0 : \alpha + 1 : 1)$

- **Points over** $\mathbb{F}_8 = \frac{\mathbb{F}_2[x]}{(x^3+x^2+1)} = \mathbb{F}_2[\omega]$

points over $\mathbb{F}_2$
$Q_1 = (\omega : \omega^2 + 1 : 1)$ $Q_2 = (\omega^2 : \omega^2 + 1 : 1)$
$Q_3 = (\omega^2 + \omega + 1 : \omega + 1 : 1)$ $Q_4 = (\omega^2 + 1 : \omega : 1)$
$Q_5 = (\omega^2 + \omega : \omega^2 : 1)$ $Q_6 = (\omega + 1 : \omega^2 + \omega + 1 : 1)$

First of all, the curve is smooth if $\mathrm{char}\,(\mathbb{F}_q) \neq 3$, as the system

$$\begin{cases} x^3 + y^3 + z^3 = 0 \\ 3x^2 = 0 \\ 3y^2 = 0 \\ 3z^2 = 0 \end{cases}$$

has no solutions in $\mathbb{P}^2$. Therefore the genus can be calculated by Plucker formula and it is equal to 1. We want to check that we did not forget any point of X. Recalling that the genus is 1, it is sufficient to calculate the number of points over $\mathbb{F}_2$. We get $N_1 = 3$, $q = 2$, $g = 2$, so $3 = 2 + 1 - (\alpha_1 + \bar{\alpha_1})$. Hence $\alpha_1 = -\bar{\alpha_1}$ and, recalling that $|\alpha_1| = \sqrt{2}$, we have $\alpha_1 = i\sqrt{2}$. So we can now compute the number of points over $\mathbb{F}_{2^r}$:

$$N_2 = 2^2 + 1 - (-2 - 2) = 9$$

$$N_3 = 2^3 + 1 - (-i\sqrt{2} + i\sqrt{2}) = 9$$

$$N_4 = 2^4 + 1 - 8 = 9.$$

So the points over $\mathbb{F}_{16}$ are those over $\mathbb{F}_4$. In general we have

$$N_r = \begin{cases} q^r + 1, & \text{if } r \text{ odd} \\ q^{2k} + 1 + (-1)^{k+1} 2^{k+1} & \text{if } r = 2k. \end{cases}$$

Let us consider now the code $C^*(X, D, G)$ where $D = P_1 + \cdots + P_8$ and $G = aP_0$ with $1 \leq a \leq 7$. The length is 8, the dimension $8 - a$ and the minimum distance is at least a. For example, if $a = 6$, $C^*(X, D, G)$ is a $[8, 2, \geq 6]$-code, while $C(X, D, G)$ is a $[8, 6, \geq 2]$-code. Now we know that $C^*(X, D, aP_0)$ is able to correct errors up to t, if $2t < d \leq a$. To correct an error of weight 2, $a = 5$ should be sufficient. But in the SV-algorithm we need a divisor A of degree at most $a - 3$ such that $\dim L(A) > 2$. But $\dim L(A) = \deg A$ so this is impossible for $a = 5$. For codes defined over this cubic curve, Lemma 3.2 gives a necessary condition. So we have to take $a = 6$. Let us find a basis of $L(aP_0)$. P_0 is in the affine plane $z = 1$, so we can

use affine coordinates and, around P_0, the curve is given by $x^3+y^3+1=0$. The tangent line in P_0 is $y+1=0$, so $v_{P_0}(x)=1$ while $v_{P_0}(y+1)=3$ (P_0 is an inflexion point). Consider the functions $x^i y^j (y+1)^{-(i+j)}$. They have a pole of order $3j+2i$ in P_0. We can easily see that the functions $f_{ij} := x^i y^j (y+z)^{-(i+j)}$ have no other poles on X, so $(f_{ij}) = -(3j+2i)P_0 + E$ with E effective divisor. We obtain that $f_{ij} \in L(G)$ if $0 \leq 3j+2i \leq a$. By choosing suitable i and j, we find a linearly independent functions in $L(aG)$, i.e. a basis of $L(aP_0)$. For instance, if $a=6$, the functions 1, $\frac{x}{y+z}$, $\frac{y}{y+z}$, $\frac{x^2}{(y+z)^2}$, $\frac{xy}{(y+z)^2}$ and $\frac{x^3}{(y+z)^3}$ form a bases of $L(6P_0)$ and they have poles of order respectively 0, 2, 3, 4, 5 and 6. Therefore, evaluating the functions in $P_1, \cdots, P_8$, a generator matrix for $C(X, D, 6P_0)$ (a check matrix for $C^*(X, D, 6P_0)$) is

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & \alpha & \alpha+1 & \alpha & \alpha+1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & \alpha+1 & \alpha \\ 1 & 1 & \alpha+1 & \alpha & \alpha+1 & \alpha & 0 & 0 \\ 1 & 0 & \alpha & \alpha+1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0. \end{pmatrix}.$$

It can be proved that there are 6 linearly independent columns, so the minimum distance is exactly 6. Let us try to decode the vector $f = c + e$ where

$$c = \begin{pmatrix} \alpha & \alpha & \alpha+1 & 1 & \alpha+1 & 1 & 0 & 0 \end{pmatrix}$$

$$e = \begin{pmatrix} \alpha & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$f = \begin{pmatrix} \alpha & \alpha & \alpha+1 & 1 & \alpha+1 & 1 & 0 & 0 \end{pmatrix}.$$

When the support of G is of the form bQ for some point G, the most natural choice for A is a divisor of the form cQ, so we can take as basis of $L(A)$ a subset of the special basis of $L(G)$. In our example we set $A = 3P_0$,$Z = 4P_0$, $Y = 3P_0$. A basis of $L(A)$ and $L(Y)$ is $\{1, \frac{x}{y+z}, \frac{y}{y+z}\}$, while $\{1, \frac{x}{y+z}, \frac{y}{y+z}, \frac{x^2}{(y+z)^2}\}$ is a basis of $L(Z)$. The matrix of the syndromes is

$$S = \begin{pmatrix} 1 \circ f & \frac{x}{y+z} \circ f & \frac{y}{y+z} \circ f \\ \frac{x}{y+z} \circ f & \frac{x^2}{(y+z)^2} \circ f & \frac{xy}{(y+z)^2} \circ f \\ \frac{y}{y+z} \circ f & \frac{xy}{(y+z)^2} \circ f & \frac{y^2}{(y+z)^2} \circ f \end{pmatrix} = \begin{pmatrix} \alpha+1 & 0 & \alpha+1 \\ 0 & 1 & 0 \\ \alpha+1 & 0 & \alpha+1 \end{pmatrix}.$$

The error locator Θ in $L(A)$ is given by $\Theta = \lambda_1 + \lambda_2 \frac{x}{y+z} + \lambda_3 \frac{y}{y+z}$ where

$$\lambda_1 \begin{pmatrix} \alpha+1 \\ 0 \\ \alpha+1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \lambda_3 \begin{pmatrix} \alpha+1 \\ 0 \\ \alpha+1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

For example we can take $\lambda_1 = \lambda_3 = 1$, $\lambda_2 = 0$, $\Theta = 1 + \frac{y}{y+z}$. Θ vanishes in P_1, P_3 and P_4, hence we have to find the unique solution of

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha+1 \\ 1 & 1 & 1 \\ 1 & \alpha+1 & \alpha \end{pmatrix} \begin{pmatrix} e_1 \\ e_3 \\ e_4 \end{pmatrix} = \begin{pmatrix} \alpha+1 \\ 0 \\ \alpha+1 \\ 1 \end{pmatrix}.$$

The unique solution is $e_1 = \alpha$, $e_3 = 1$, $e_4 = 0$. We conclude that

$$e = \begin{pmatrix} \alpha & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

3.3 The Duursma algorithm

In the SV-algorithm we looked for an error locator Θ in $L(A)$ and, in order to find it, we needed another auxiliary divisor Y. The syndromes for products between functions in $L(A)$ and $L(Y)$ could be calculated from the received vector if $Y + A \preceq G$. But from this condition we get the restriction $\deg G \geq 3g + 2t - 1$. We will describe soon how this restriction can be overtaken by the so-called majority voting method. Roughly speaking, it allows to deduce further syndromes of e from the known ones, calculated from f.
Let $C^*(X, D, G)$ be as usual. This code can correct errors of weight up to t, where $2t \leq \deg G - 2g + 1$. Take a point Q which is not in the support of D. Put $G' = G - (\deg G - 2g + 1)Q$. $G' \preceq G$, so $C^*(X, D, G) \subseteq C^*(X, D, G')$ and $\deg G' = 2g + 2t - 1$. Choose a divisor A with $\deg A = t$ and support disjoint from that of D. Define $A' = G' - A - (2g - 1)Q$. Also $\deg A' = t$. Our strategy is to find an error locator in the space $L(A+rQ)$ or $L(A'+rQ)$ with $r \leq 2g - 1$ and r as small as possible. For sure it can be done since, by Proposition 3.1, there exists an error locator in $L(A+gQ)$, as $\deg(A+gQ) = t + g$ and $\dim L(A + gQ) \geq t + 1$. Moreover, Proposition 3.3 tells we can calculate it by using the syndromes for products of functions in $L(A + gQ)$ and $L(A' + (2g - 1)Q)$.

Definition 3.3 *Let Q be a rational point of the curve X. For any divisors H and any non-zero function Θ, the H-**order** of Θ with respect to Q is the smallest integer m such that Θ belongs to $L(H + (m - \deg H)Q)$, if such an integer exists. Otherwise the H-order is defined to be $+\infty$. The H-order of Θ with respect to Q is denoted by $\mu_{H,Q}(\Theta)$ (or simply $\mu_H(\Theta)$ when Q does not change).*

Proposition 3.4 *Let Q be a fixed rational point. The following properties hold for divisors H, H' and non-zero functions Θ, Θ':*

1. *Let $\mu_H(\Theta) = r < \infty$. Then $r \geq 0$ and $v_Q(\Theta) = d(H) - H(Q) - r$, where $H(Q)$ is the coefficient of Q in H.*

2. *Let $H < K$ and $\mu_H(\Theta) = r < \infty$. Then $\mu_K(\Theta) = r + \deg(K - H) - (K - H)Q$, where $(K - H)Q$ is the coefficient of Q in $K - H$.*

3. *If $\mu_H(\Theta) = r < \infty$ and $\mu_{H'}(\Theta') = r' < \infty$, then $\mu_{H+H'}(\Theta\Theta') = r + r'$.*

Proof:

1. By contradiction we assume $r < 0$. Then $\Theta \in L(H + (r - \deg H)Q)$. But $\deg(H + (r - \deg H)Q) = r < 0$ and so $L(H + (r - \deg H)Q) = \{0\}$. Therefore $\Theta = 0$, which is a contradiction because $\Theta \neq 0$ by hypothesis. By definition of H-order, Θ belongs to $L(H+(r-\deg H)Q)$ but it is not in $L(H + (r - \deg H)Q)$. It means that $(\Theta) + H + (r - \deg H)Q \succeq 0$ but $(\Theta) + H + (r - 1 - \deg H)Q \not\succeq 0$. Hence $v_Q(\Theta) + H(Q) + r - \deg H \geq 0$ but $v_Q(\Theta) + H(Q) + r - 1 - \deg H < 0$. We finally have that $\mu_K(\Theta) = r + \deg(K - H) - (K - H)Q$.

2. If $\Theta \in L(H + kQ)$ then $\Theta \in L(K + kQ)$, so $\mu_K(\Theta) < \infty$. By part (1), we obtain $\mu_K(\Theta) = \deg K - K(Q) - v_Q(\Theta) = \deg(K - H) + \deg H - (K - H)Q - H(Q) - v_Q(\Theta) = r + \deg(K - H) - (K - H)Q$.

3. By definition of order, $\Theta \in L(H + (r - \deg H)Q)$ and $\Theta' \in L(H' + (r\prime - \deg H')Q)$. Since $(\Theta\Theta') = (\Theta) + (\Theta')$, we have $\Theta\Theta' \in L(H + H' + (r + r' - \deg H - \deg H')Q) = r + r'$. Hence $\mu_{H+H'}(\Theta\Theta') < +\infty$ and so we can apply point (1). Recalling that $v_Q(\Theta\Theta') = v_Q(\Theta) + v_Q(\Theta')$, we obtain $\mu_{H+H'}(\Theta\Theta')$. □

Corollary 3.2 *Let $\psi_1, \cdots, \psi_m$ be functions such that $\mu_H(\psi_1) < \cdots < \mu_H(\psi_m)$ is a complete list of the possible values $\mu_H(\psi) \leq \deg H + r$. Then $\{\psi_1, \cdots, \psi_m\}$ is a basis of $L(H + rQ)$.*

The main object involved in the Duursma algorithm is the syndromes table S. As in the SV-algorithm, suppose a word c is transmitted and $f = c + e$ is received, where e is an error vector of weight not bigger than t. Using the previous corollary, we can choose bases ϕ_k of $L(A + A' + (3g - 1)Q)$, ψ_i of $L(A + (2g - 1)Q)$ and χ_j of $L(A' + (2g - 1)Q)$, where $\mu_{A+A'}(\phi_k) = k$, $\mu_A(\psi_i) = i$ and $\mu_{A'}(\chi_j) = j$. We use the A-order to index the rows and the A' for the columns. We call these indices the **orders of the rows and the columns**. S is defined by

$$S_{ij} = \psi_i \chi_j \circ e$$

and so S is a $(t + g) \times (t + g)$ matrix. By Proposition 3.4, the $(A + A')$-order of the (i, j)-entry is $i + j$. The knowledge of S is sufficient to find an error locator. In fact by Corollaries 3.2 and 3.1, knowing the rows $1, \cdots, i$ means knowing all the syndromes $\psi\chi$, where $\psi \in L(A + (i - t)Q)$, $\chi \in L(A' + (2g - 1)Q)$. If there exists ψ such that $\psi\chi \circ e = 0$ for every χ, then ψ is an error locator in $L(A + (i - t)Q)$. Thus we can check if an error locator

in $L(A+(i-t)Q)$ exists. Analogously for columns up to order j to find an error locator in $L(A'+(j-t)Q)$. The fundamental problem is that we do not know e, but we have just f, so we cannot calculate all the syndromes in S.

Nevertheless, observe that $\phi_i\chi_j$ belongs to $L(A+A'+(i+j-2t)Q) = L(G+(i-j-\deg G)Q)$, so if $i+j\deg G$, then $G+(i+j-\deg G)Q \preceq G$ and $\psi_i\chi_j \circ e = \psi_i\chi_j \circ f$, hence the entries of order up to $\deg G$ are known.

Let us say that a row (or column) is known if all the entries in that row (or column) are known, unknown otherwise. By construction, the orders of rows and columns are less or equal $2g-1+t$, so the rows and columns of order at most t are known, as, for their (i,j)-entries, we have $i+j \leq t+2g-1+t = 2g-2t-1 \leq \deg G$.

There exists in every row an element with A'-order equal to $2g-1+t$, so, if $i > t+\deg G-(2g+2t-1)$, the row is initially unknown. The order of the t-th row is at most $t+g-1$.

If $\deg G \geq 3g+2t-1$ then for the (i,j)-entries in the first t rows, we have $i+j \leq t+g-1+2g-1+t = 2t+3g-2 < \deg G$, so the first t rows are known. In this case these rows form the syndrome table used by the SV processor with auxiliary divisors $A+rQ$ and $A'+(2g-1)Q$, where $r+t$ is the order of the t-th row. The first t rows can be known even if $\deg G < 3g+2t-1$.

It can happen that, from the known rows and columns, we cannot find any error locator. This case is more interesting because we have to use a technique called *majority voting* in order to deduce more syndromes from the known entries. As a preliminary remark, the next lemma shows how, from a new entry, we can obtain many others.

Lemma 3.3 *Suppose all the syndromes $\phi \circ e$ are known, for $\mu_{A+A'}(\phi) < s$, and an entry of order s is known. Then all the entries of order s are known.*

Proof: Let S_{ij} be the known entry of order s. It means that $i+j=s$ and $S_{ij} = \psi_i\chi_j \circ e$. $\psi_i\chi_j \in L(A+A'+(s-2t)Q)$, so it can be written as $a\phi_s+\phi'$, where $a \in \mathbb{F}_q$, $\mu_{A+A'}(\phi') < s$. $S_{ij} = a\phi_s \circ e + \phi' \circ e$ and $\phi' \circ e$ is known by hypothesis, hence we can calculated $\phi_s \circ e$. By linearity we can deduce the syndromes of the functions in $L(A+A'+(s-2t)Q)$, hence every entry of order s. □

Motivated by the proof of the lemma, it is convenient to write every product $\psi_i\chi_j$ with $i+j > \deg G$ as a linear combination of the ϕ_i's. Moreover, we can stop when $i+j > 3g-1+2t$, because, in the worst case, we will find an error locator in $L(A+gQ)$, so we will work with function of $(A+A')$-order at most $3g-1+2t$.

We recall that our aim is to find an error locator Θ with $\mu_A(\Theta) = u$ or $\mu_{A'}(\Theta) = u$ and we want u as small as possible, since finding an error

locator with $\mu_A(\Theta)$ requires the knowledge of the rows with order up to u. The following proposition describes how the increasing rate of the number of error locators depends on u.

Proposition 3.5 *Let e have weight at most $t = \deg A = \deg A'$ and let $t \le u \le g+t$. Suppose there are no error locators Θ for e with $\mu_A(\Theta) < u$ or $\mu_{A'}(\Theta) < u$. For r between u and $2g-1+t$, let r' be the value $2g-1+t+u-r$. Let p be the number of r between u and $2g_1 + t$ such that there are error locators Θ, η for e with $\mu_A(\theta) = r$ and $\mu_{A'}(\eta) = r'$, and let q be the number of r between u and $2g - 1 + t$ such that there is neither an error locator Θ with $\mu_A(\theta) = r$ nor an error locator η with $\mu_{A'}(\eta) = r'$. Then $p - q \ge u - t$.*

Proof: First remark that, for r running in the interval $[u, 2g-1+t]$, also r' does the same, and their sum is constantly equal to $2g - 1 + t + u$. Define

$$J = \{r \mid u \le y \le 2g - 1 + t\},$$

$$I = \{r \in J \mid \text{there exists an error locator with } A\text{-order} r\},$$

$$I' = \{r \in J \mid \text{there exists an error locator with } A'\text{-order } r'\}.$$

We get

$$p = \#(I \cap I')$$

$$q = \#(J \setminus (I \cup I')) = 2g + t - u - \#(I \cup I').$$

We claim that both $\#I$ and $\#I'$ are greater or equal t.

Put $D_e = \sum_{e_i \neq 0} P_i$, i.e. the sum of the error locations. An error locator in $L(A+(r-t)Q)$ is an element of $L(A+(r-t)Q-B_e)$. Consider $r = 2g-1+t$. We have to study $L(A+(2g-1)Q-B_e)$. We have $\deg(A+(2g-1)Q-B_e) \ge 2g-1$, so $\dim L(A+(2g-1)Q-B_e) \ge g$. By Corollary 3.2 we can choose a basis of $L(A+(2g-1)Q-B_e)$ by choosing ρ_i with different $\mu_{A-B_e}(\rho_i) = i$ and $\mu_{A-B_e}(\rho_i) \le 2g-1+t-\deg B_e$. Recalling that $\mu_A(\rho_i) \ge u$ because there are no error locators with A-order less than u, we get, by Proposition 3.4(b), $\mu_{A-B_e}(\rho_i) = i + \deg B_e \le 2g_1 + t$. We found at least g error locators with different orders between u and $2g-1+t$. Thus $\#I \ge g$.

Arguing analogously on the columns, we get $\#I' \ge g$. □

A fundamental role in the algorithm we are explaining is played by row and column candidates. We know that, in order to find an error locator with A-order r, we test a function ψ with all the functions in $L(A'+(2g-1+t)Q)$. More explicitly, if S^i is the i-th row of S, we look for $\sum_{i \le r} a_i \psi_i$, where $\sum_{i \le r} S^i = 0$. But many times we know just the syndromes for the products with function of A'-order up to r', so we can test ψ just with functions in $L(A'+(r'+t)Q)$. If $r' < 2g-1+t$ we are not sure ψ is an error locator. It is just a possible candidate. This motivates the formal definition below.

Definition 3.4 *A function θ is called a* ***row candidate*** *of order (r, r') if $\mu_A(\Theta) = r$ and $\Theta\eta \circ e = 0$ for all the functions η with $\mu_{A'}(\eta) \leq r'$. We say Θ to be* ***normalized*** *if $\Theta = \psi_r + \Theta'$, with $\mu_A(\Theta') < r$.*

A function θ is called a ***column candidate*** *of order (r, r') if $\mu_{A'}(\eta) = r$ and $\Theta\eta \circ e = 0$ for all the functions Θ with $\mu_A(\Theta) \leq r$. η is* ***normalized*** *if $\eta = \chi_{r'} + \eta'$, with $\mu_{A'}(\eta') < r'$.*

REMARKS: We said above that a row candidate of order $(r, 2g - 1 + t)$ is an error locator. Clearly a row candidate of order (r, r') is, a fortiori, a row candidate of order (r, r'') for every $r'' < r'$. Similarly for column candidates.

The following proposition shows how to find candidates, and their relations with the syndromes matrix. We will state it just for row candidates. Corresponding properties hold for column candidates.

Proposition 3.6 *1. Let $S_{|rr'}$ be the matrix $(S_{ij})_{i\leq r, j\leq r'}$. A function $\sum_{i\leq r} a_i\psi_i$ with $a_i \neq 0$ is a row candidate of order (r, r') if and only if $\sum_{i\leq r} S^i = 0$, where S^i is the i-th row of $S_{|rr'}$.*

2. If Θ is a normalized row candidate of order $(r, r' - 1)$ and η is a normalized column candidate of order $(r - 1, R')$, then

$$\Theta\chi_{r'} \circ e = \psi_r\eta \circ e.$$

3. If θ_1 and Θ_2 are distinct normalized row candidates of order $(r, r' - 1)$ and $\Theta_1\chi_{r'} \circ e \neq \Theta_2\chi_{r'} \circ e$, then there are no column candidates of order $(r - 1, r')$.

Proof:

1. It follows directly from Corollary 3.2 and the linearity of the syndrome with respect to the functions.

2. Write $\Theta = \psi_r + \Theta'$ with $\mu_A(\Theta') < r$, $\eta = \chi_{r'} + \eta'$ with $\mu_{A'}(\eta') < r'$. We get $\Theta\chi_{r'} \circ e = \Theta\eta \circ e - \Theta\eta' \circ e = \Theta\eta \circ e = \psi_r\eta \circ e + \Theta'\eta \circ e = \psi_r\eta \circ e$.

3. By contradiction, assume there exists a column candidate of order $(r - 1, r')$. Then, by (2), $\Theta_1\chi_{r'} \circ e = \psi_r\eta \circ e = \Theta_2\chi_r \circ e$, which is a contradiction. □

We are now ready to learn how to add new syndromes in the matrix S. Suppose all the syndromes $\varphi \circ e$ are known for $\mu_{A+A'}(\varphi) < s$, but $\varphi_s \circ e$ is unknown. This implies that all the entries of order less than s are known,

but no one of order s. In this case $s \geq \deg G + 1 \geq 2t + 2g$. Suppose moreover that the known rows and column did not give any error locator. We consider now all the entries $S_{rr'}$ where $r + r' = s$. Since all the entries in $S_{|r,r'-1}$ and $S_{|r-1,r'}$ are known, we are able to decide whether there are a row candidate Θ of order $(r, r' - 1)$ and a column candidate η of order $(r - 1, r')$. If both exist, we can choose them normalized and we shall call $S_{rr'}$ a **test entry** for s. Note that the value $\Theta\chi_{r'} \circ e$ is independent by the the chosen row candidate.

If there exists an error locator with A-order r, we can guess it is exactly Θ. In this case $\Theta \circ e = 0$. But $\theta = \psi_r + \Theta'$, so $0 = \Theta\chi_{r'} \circ e = \psi_r\chi_{r'} \circ e + \Theta'\chi_{r'} \circ e$. Thus $\psi_r\chi_{r'} \circ e = -\Theta'\chi_{r'} \circ e$, where the right hand side is known, as $\mu_{A+A'}(-\Theta'\chi_{r'}) < s$. The proof of Lemma 3.3 shows how it is possible to deduce from $\psi_r\chi_{r'} \circ e$ the value of $\varphi_s \circ e$. Let us call this value the **vote of the entry** $S_{rr'}$. As consequence of the previous proposition, observe that the same vote for $S_{rr'}$ could be obtained by supposing η to be an error locator.

We are not sure this vote is the true value of $\varphi_s \circ e$, since it comes from the guess $\Theta \circ e = 0$. Nevertheless, the next proposition ensures that the majority of votes are correct.

Proposition 3.7 *The number of test entries $S_{rr'}$ with $r + r' = s$ producing correct votes exceeds those producing incorrect votes by at least $s - 2g - 2t + 1 > 0$. In particular there is at least one of such a test entry.*

Proof: Let $u = s - 2g - t + 1$. As $s \geq 2g + 2t$, $u \geq t + 1$ and we are allowed to apply Proposition 3.5. If r' is defined as in there, the pairs (r, r') are exactly those such that $r + r' = s$. We claim that the number of correct votes is at least p and the number of incorrect votes is at most q.

Suppose there exist error locators Θ, η with $\mu_A(\Theta) = r$ and $\mu_{A'}(\eta) = r'$. We can suppose them normalized. Θ is also a row candidate of order $(r, r'-1)$ and η is a column candidate of order $(r - 1, r')$, so, for each normalized row candidate Θ_1 of order $(r, r' - 1)$, $\Theta_1\chi - r' \circ e = \Theta\chi - r' \circ e = 0$. It means the vote of $S_{rr'}$ was correct.

On the other hand, suppose $S_{rr'}$ gives an incorrect vote, i.e. there exist a normalize row candidate Θ_1 of order $(r, r' - 1)$, a column candidate η_1 of order $(r - 1, r')$ and $\Theta_1\chi_{r'} \circ e \neq 0$. Suppose by contradiction there exists an error locator θ with $\mu_A(\theta) = r$. Then $0 = \Theta\chi_{r'} \circ e = \Theta_1\chi_{r'} \circ e \neq 0$. For similar reasons it is impossible there exist an error locator with A'-order equal to r'.

We finally obtain that the difference between correct and incorrect votes is at least $p - q \geq u - t = s - 2g - 2t + 1$. □

REMARK: The existence of a basis element φ_s for $s \geq 2t + 2g$ implies that there is an entry of order s in S. Indeed φ_s can be chosen as a product $\psi_r\chi_{r'}$.

Let us write now the Duursma algorithm.

DUURSMA ALGORITHM: Let c be a word of the code $C^*(X, D, G)$, based on a curve X of genus g and let $f = c + e$ be the received word, where $wt(e) \leq t$ and $\deg G \geq 2t + 2g - 1$.

STEP 0: Preliminary step
This step is done just once for every fixed code. Choose a divisor A with $\deg A = t$ and support disjoint from the one of D. Pick a rational point Q not in the support of D. Put $G' = G - (\deg G + 2g + 2t - 1)Q$ and $A' = G' - A - (2g - 1)Q$. Choose bases $\{\varphi_0, \cdots, \varphi_{3g+2t-1}\}$ of $L(A + A' + (3g - 1)Q)$, $\{\psi_0, \cdots, \psi_{2g+t-1}\}$ of $L(A + (3g - 1)Q)$ and $\{\chi_0, \cdots, \chi_{2g+t-1}\}$ of $L(A' + (2g - 1)Q)$, indexed respectively by the $(A + A')$, A and A' orders. For all indexes i, j with $\deg G < i + j \leq 3g + 2t - 1$ write $\psi_i\chi_j$ as a linear combination of $\varphi_0, \cdots, \varphi_{i+j}$.

STEP 1: Syndrome calculation
Construct the syndromes table S in the following way: S is a $(t+g) \times (t+g)$ matrix where rows and columns are indexed by A-orders and A'-orders. For $i + j \leq \deg G$, $S_{ij} = \psi_i\chi_j \circ f$. If all the syndromes are 0, then f belongs to $C^*(X, D, G)$. Leave the cells of order greater than $\deg G$ blank. Calculate the syndromes $\varphi_s \circ f$ for $s \leq \deg G$.

STEP 2: Test for error locator
Let u be the maximal order of the known rows. Look for a non-zero solution of the linear system

$$\sum_{i \leq u} \alpha_i S^i = 0$$

where S^i is the i-th row of S. If a solution α exists, then $\sum_{i \leq u} \alpha_i \psi_i$ is an error locator: go to step 5.
Let u be the maximal order of the known columns. Look for a non-zero solution of the linear system

$$\sum_{j \leq u} \beta_j S_j = 0$$

where S_j is the j-th column of S. If a solution β exists, then $\sum_{j \leq u} \beta_j \chi_j$ is an error locator: go to step 5.

STEP 3: Estimate additional syndromes
Assume that every entry of order $s - 1$ is known, while no entry of order s is

known. For each pair (r, r') with $r + r' = s$, try to solve the linear systems

$$\sum_{i<r} S_{ik}\alpha_i = -S_{rk} \qquad \text{for } k < r'$$

$$\sum_{j<r'} S_{kj}\beta_j = -S_{kr'} \qquad \text{for } k < r.$$

If both solutions α and β exist, put $S_{rr'} = -\sum_{i<r} \alpha_i S_{ir'} = -\sum_{j<r'} \beta_j S_{rj}$. and call $S_{rr'}$ a test entry for s.

STEP 4: Majority voting
For each test entry $S_{rr'}$ use the expressions of $\psi_r\chi_{r'}$ in terms of the basis φ_i, and the known syndromes $\phi_i \circ e$ for $i < s$, to calculate the vote $\varphi_s \circ e$. The true value $\varphi_s \circ e$ is the vote that occurs most frequently. Using this value, recalculate all the syndromes $\psi_r\chi_{r'}$ (all but the test entries that gave correct votes). If an additional column or row is known, go to step 2, otherwise go to step 3.

STEP 5: Find error locations
We found an error locator Θ with $\mu_A(\Theta) \leq t + g$ or $\mu_{A'}(\Theta) \leq t + g$. Determine the set $M = \{P_i \in supp(D) \mid \Theta(P_i) = 0\}$. This set contains the error locations.

STEP 6: Calculation of error values
Suppose we found an error locator using rows (or columns) up to order u. Then the syndromes $\varphi_k \circ e$ for $k \leq u + 2g + t - 1$ are known. Solve the equations

$$\sum_{P_l \in M} \varphi_k(P_l)e_l = \varphi_k \circ e \qquad \text{for } k \leq u + 2g + t - 1.$$

Extend the unique solution $(e_l : P_l \in M)$ of this set of equations by putting $e_l = 0$ for $P_l \notin M$. Then $e = (e_1, \cdots, e_n)$ is the error vector.

REMARK: The uniqueness of the solution in step 6 follows from Theorem 3.1 with divisors $A + (u - t)Q$ and $A + A' + (u + 2g + t - 1 - 2t)Q$.

3.4 Example

Let us go back to the code $C^*(X, D, G)$, where X is the curve $x^3+y^3+z^3 = 0$, $P_0 = (0 : 1 : 1)$, G is the sum of the other point over $\mathbb{F}_4$ and $D = aP_0$. In subsection 3.2 we said that the SV-algorithm requires $a \geq 6$ to correct an error of weight 2. We shall take $a = 5$ and use the Duursma algorithm.

Suppose we received $f = x + e$, where

$$\begin{aligned} x = &\quad (\ \alpha \quad \alpha+1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0\ ) \\ e = &\quad (\ \alpha \quad\ 0 \quad\ 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0\ ) \\ f = &\quad (\ 0 \quad \alpha+1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0\ ). \end{aligned}$$

We chose a word x in $C^*(X, D, 5P_0)$ but not in $C^*(X, D, 6P_0)$. The natural choices in the preliminary step are $Q = P_0$ and $A = 2P_0$, so all the bases can be chosen as subsets of the single basis of $L(6P_0) = L(A + A' + (2g-1)P_0)$. We get $A' = A = 2P_0$ and bases

$$\{\varphi_0 = 1, \varphi_2 = \frac{x}{y+z}, \varphi_3 = \frac{y}{y+z}, \varphi_4 = \frac{x^2}{(y+z)^2}, \varphi_5 = \frac{xy}{(y+z)^2}, \varphi_6 = \frac{x^3}{(y+z)^3}\},$$

$$\{\psi_0 = \varphi_0, \psi_2 = \varphi_2, \psi_3 = \varphi_3\},$$

$$\{\chi_0 = \varphi_0, \chi_2 = \varphi_2, \chi_3 = \varphi_3\}$$

In the syndromes table S we know all the entries of order at most 5. Just S_{33} is unknown. Write $\psi_e \chi_3 = \varphi_6$. The syndromes table is

$$S = \begin{pmatrix} \alpha+1 & 1 & \alpha+1 \\ 1 & 0 & 1 \\ \alpha+1 & 1 & \end{pmatrix}.$$

Observe that S is symmetric, so working with rows or columns gives the same final result. The system

$$\alpha_1 \begin{pmatrix} \alpha+1 \\ 1 \\ \alpha+1 \end{pmatrix} + \alpha_2 \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

has just a trivial solution, so there are not locators with A-order 2. The only entry of order 6 is S_{33}, so it must be a test entry by Proposition 3.7, i.e. there must be a row candidate of order $(3, 2)$. Indeed a solution for

$$\alpha_0 \begin{pmatrix} \alpha+1 \\ 1 \end{pmatrix} + \alpha_2 \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha+1 \\ 1 \end{pmatrix}$$

is given by $\{\alpha_0 = 1, \alpha_2 = 0\}$, so $S_{33} = S_{03} = \alpha + 1$. This is the only vote, hence it must be correct. The syndromes matrix is now

$$S = \begin{pmatrix} \alpha+1 & 1 & \alpha+1 \\ 1 & 0 & 1 \\ \alpha+1 & 1 & \alpha+1 \end{pmatrix}.$$

A new row has been found and the matrix is totally known, so there must be an error locator. We now remark that $\{\alpha_0 = 1 = \alpha_3, \alpha_2 = 0\}$ is a solution for the system

$$\alpha_0 \begin{pmatrix} \alpha+1 \\ 1 \\ \alpha+1 \end{pmatrix} + \alpha_2 \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + \alpha_3 \begin{pmatrix} \alpha+1 \\ 1 \\ \alpha+1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

hence $\Theta = \psi_0 + \psi_3 = 1 + \frac{y}{y+z}$ is an error locator for e. It vanishes in P_1, P_3 and P_4. We have to solve the system

$$\varphi_k(P_1)e_1 + \varphi_k(P_3)e_3 + \varphi_k(P_4)e_4 = \varphi_k \circ e \quad \text{for } k \leq 6.$$

It is easy to see that $\{e_1 = \alpha, e_3 = 0, e_4 = 1\}$ is the only solution for

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha+1 \\ 1 & 1 & 1 \\ 1 & \alpha+1 & \alpha \\ 1 & \alpha & \alpha+1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} e_1 \\ e_3 \\ e_4 \end{pmatrix} = \begin{pmatrix} \alpha+1 \\ 1 \\ \alpha+1 \\ 0 \\ 1 \\ \alpha+1 \end{pmatrix}.$$

Therefore we obtain

$$e = \begin{pmatrix} \alpha & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

3.5 Another example: the Klein quartic

The previous example does not show explicitly the majority voting mechanism. To emphasize it, we have to consider an example such that the syndromes matrix contains a larger number of unknown entries.

The curve X defined by $x^3y + y^3z + xz^3 = 0$ is called the *Klein quartic*. X, over a field with characteristic different from 7, is smooth, so its genus can be easily calculated by the Plücker formula and it equals 3. We shall often work with $\mathbb{F}_2$ and its algebraic extensions. The point of the Klein quartic over $\mathbb{F}_2$ are:

$$P_0 = (0:0:1) \qquad P_1 = (0:1:0) \qquad P_2 = (1:0:0).$$

Let $\mathbb{F}_{16}$ the field of 16 elements, based on the irreducible polynomial $x^4 + x^3 + 1$. For short, every element y of this field will be denoted by an integer n between 0 and 15, such that, if $(a_3, a_2, a_1, a_0)_2$ is the binary representation of n, then $y = a_3x^3 + a_2x^2 + a_1x + a_0$ in $\mathbb{F}_2[x]/(x^4 + x^3 + 1)$.

The points of the Klein quartic over $\mathbb{F}_{16}$ are those over $\mathbb{F}_2$ and

$$P_3 = (10 : 11 : 1) \qquad P_4 = (11 : 10 : 1)$$

$$P_5 = (3 : 10 : 1) \quad P_6 = (5 : 11 : 1) \quad P_7 = (8 : 10 : 1) \quad P_8 = (15 : 11 : 1)$$

$$P_9 = (10 : 2 : 1) \quad P_{10} = (11 : 4 : 1) \quad P_{11} = (10 : 9 : 1) \quad P_{12} = (11 : 14 : 1)$$

$$P_{13} = (6 : 8 : 1) \quad P_{14} = (13 : 15 : 1) \quad P_{15} = (7 : 3 : 1) \quad P_{16} = (12 : 5 : 1).$$

The points in the same row are conjugate. P_3 and P_4 are over $\mathbb{F}_4$ (they are rational points of degree 2 over $\mathbb{F}_2$).

Consider the codes $C^*(X, D, aP_0)$, where $D = P_1 + \cdots + P_{16}$ and $5 \leq a \leq 15$. They have dimension $18 - a$ and minimum distance greater or equal $a - 4$. In this example we want to correct errors of weight at most 3, so we need $a \geq 11$.

The function z/x has a pole of order 3 in P_0, while y/z has a zero of multiplicity 1 in P_0. In the following table the functions forming a base for $L(16P_0)$ and their pole orders in P_0.

pole ord.	0	3	5	6	7	8	9	10	11	12	13	14	15	16
function	1	$\frac{z}{x}$	$\frac{yz}{x^2}$	$\frac{z^2}{x^2}$	$\frac{y^2z}{x^3}$	$\frac{yz^2}{x^3}$	$\frac{z^3}{x^3}$	$\frac{y^2z^2}{x^4}$	$\frac{yz^3}{x^4}$	$\frac{z^4}{x^4}$	$\frac{y^2z^3}{x^5}$	$\frac{yz^4}{x^5}$	$\frac{z^5}{x^5}$	$\frac{z^6}{x^6}$

We want to decode $f = x + e$, where $x \in C^*(X, D, 11P_0)$ and e is the error vector. For example assume

$$\begin{aligned} f = &\ (1\ 1\ 10\ 11\ 3\ 5\ 8\ 15\ 11\ 10\ 11\ 10\ 0\ 0\ 0\ 0) \\ g = &\ (0\ 0\ 0\ 11\ 0\ 6\ 4\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0)\ . \\ e = &\ (1\ 1\ 10\ 0\ 3\ 3\ 8\ 11\ 11\ 10\ 11\ 10\ 0\ 0\ 0\ 0) \end{aligned}$$

The natural choice for Q and A is $Q = P_0$, $A = 3P_0$. Thus $A' = A$. As bases of $L(14P_0) = L(A + A' + (3g - 1)P_0)$ we choose the functions φ of the basis of $L(16P_0)$ with A-order up to 14. The functions among them with order at most 8 form a basis for $L(A + (2g - 1)P_0) = L(A' + (2g - 1)P_0) = L(8P_0)$. With respect to these choices, we get the syndromes table

$S =$

	0	**3**	**5**	**6**	**7**	**8**
0	9	5	0	11	2	7
3	5	11	7	5	7	15
5	0	7	7	15		
6	11	5	15			
7	2	7				*
8	7	15			*	*

where the number in bold are the orders of rows and column.

Observe that S is symmetric, so working with rows or columns gives the same final result. Since the rows 0 and 3 are linearly independent, we are not able to find an error locator; hence we have to go to the third step of the Duursma algorithm and to add more syndromes in the matrix. There are 3 entries of order 12, namely S_{57}, S_{66} and S_{75}. Consider S_{66}. Hence $\{a_0 = 11, a_3 = 12, a_5 = 0\}$ is a non-zero solution for

$$a_0 \begin{pmatrix} 9 \\ 5 \\ 0 \end{pmatrix} + a_3 \begin{pmatrix} 5 \\ 11 \\ 7 \end{pmatrix} + a_5 \begin{pmatrix} 0 \\ 7 \\ 7 \end{pmatrix} = \begin{pmatrix} 11 \\ 5 \\ 15 \end{pmatrix}$$

so there exists a row candidate of order $6, 5$ and, by symmetry, a column candidate of order $(5, 6)$. S_{66} is a test entry and its vote is given by $S_{66} = 11 \cdot 11 + 5 \cdot 12 = 4$. Now take S_{57}. We have

$$3 \begin{pmatrix} 9 \\ 5 \end{pmatrix} + 13 \begin{pmatrix} 0 \\ 7 \end{pmatrix} = \begin{pmatrix} 2 \\ 7 \end{pmatrix},$$

$$11 \begin{pmatrix} 9 \\ 5 \\ 0 \\ 11 \end{pmatrix} + \begin{pmatrix} 5 \\ 11 \\ 7 \\ 5 \end{pmatrix} = \begin{pmatrix} 0 \\ 7 \\ 7 \\ 15 \end{pmatrix};$$

hence S_{57} is a test entry with vote $8 = 11 \cdot 2 + 7 = 3 \cdot +13 = 13 \cdot 7$. By symmetry, also S_{75} gives the same vote. Therefore the true value of $\varphi_{12} \circ e$ is 8. The new syndromes table is

$S =$

	0	**3**	**5**	**6**	**7**	**8**
0	9	5	0	11	2	7
3	5	11	7	5	7	15
5	0	7	7	15	8	
6	11	5	15	8		
7	2	7	8			*
8	7	15			*	*

.

No new rows have been added, so we have to calculate $\varphi_{13} \circ e$. The entries of order 13 are S_{58}, S_{67}, S_{85} e S_{76}. Since S is symmetric we can reduce to study S_{58} and S_{67}. Let us start with the first one. The system

$$a_0 \begin{pmatrix} 9 \\ 5 \\ 0 \\ 11 \\ 2 \end{pmatrix} + a_3 \begin{pmatrix} 5 \\ 11 \\ 7 \\ 5 \\ 7 \end{pmatrix} = \begin{pmatrix} 0 \\ 7 \\ 7 \\ 15 \\ 8 \end{pmatrix}$$

has the non-zero solution $\{a_0 = 11, a_3 = 1\}$, so there exists a row candidate of order $(5, 7)$, namely $11\psi_0 + \psi_3$. It can be calculated that there exists also a column candidate of order $(3, 8)$, hence the $(5, 8)$-entry is a test entry with vote $S_{58} = 11 \cdot 7 + 15 = 12$. As consequence of majority voting system, either $(6, 7)$ is not a test entry or it gives the same vote as $(5, 7)$. Indeed the system

$$a_0 \begin{pmatrix} 9 \\ 5 \\ 0 \\ 11 \end{pmatrix} + a_3 \begin{pmatrix} 5 \\ 11 \\ 7 \\ 5 \end{pmatrix} + a_5 \begin{pmatrix} 0 \\ 7 \\ 7 \\ 15 \end{pmatrix} = \begin{pmatrix} 11 \\ 5 \\ 15 \\ 8 \end{pmatrix}$$

does not have any solution different from 0, so no row candidate of order $(6, 6)$ exists. We conclude that $\varphi_{13} \circ e = 12$ and the table is now

$S =$

	0	**3**	**5**	**6**	**7**	**8**
0	9	5	0	11	2	7
3	5	11	7	5	7	15
5	0	7	7	15	8	12
6	11	5	15	8	12	
7	2	7	8	12		*
8	7	15	12		*	*

We added a new row, namely S^5, so we have to go back to step 2 of the algorithm and check if $a_0 S^0 + a_3 S^3 + a_5 S^5 = 0$ has a non-zero solution. A solution is $\{a_0 = 11, a_3 = a_5 = 1\}$ and it implies that $\Theta = 11\psi_0 + \psi_3 + \psi_5$ is an error locator for e. Θ, applied in $P_1, \cdots, P_{16}$ is

$$\begin{pmatrix} 11 & 11 & 1 & 0 & 1 & 0 & 1 & 0 & 13 & 6 & 12 & 7 & 8 & 14 & 3 & 4 \end{pmatrix}.$$

The error locations are among P_4, P_6 and P_8. The error vector can be calculated by finding the unique solution for

$$\varphi_k(P_4)e_4 + \varphi_k(P_6)e_6 + \varphi_k(P_8)e_8 = \varphi_k \circ e \qquad \text{for } k \leq 13.$$

It means to solve

$$\begin{pmatrix} 1 & 1 & 1 \\ 10 & 15 & 5 \\ 1 & 4 & 14 \\ 11 & 3 & 8 \\ 11 & 6 & 7 \\ 10 & 14 & 4 \\ 1 & 8 & 3 \\ 1 & 9 & 2 \\ 11 & 12 & 13 \\ 10 & 5 & 15 \\ 10 & 10 & 10 \end{pmatrix} \begin{pmatrix} e_4 \\ e_6 \\ e_8 \end{pmatrix} = \begin{pmatrix} 9 \\ 5 \\ 0 \\ 11 \\ 2 \\ 7 \\ 5 \\ 7 \\ 15 \\ 8 \\ 12 \end{pmatrix}.$$

The unique solution is $\{e_4 = 11, e_6 = 6, e_8 = 4\}$, as we wanted.

4 Codes over higher dimensional varieties

After talking about AG codes over curves, we want to define AG codes over higher dimensional varieties. In order to pass to higher dimensional varieties we need the tools of modern algebraic geometry and, in particular, scheme-theory. Therefore, the first part will be spent to introduce (or recall) the necessary definitions and basic facts from algebraic geometry. To do this we will follow [7] quite closely and we will often refer to it for proofs and deeper information. We assume the main properties of schemes and morphisms of schemes to be known. In subsection 4.3 codes over varieties are defined using the H-construction introduced by Tsfasman and Vladut in [21].

4.1 Sheaves of modules

Definition 4.1 *Let $(X, \mathcal{O}_X)$ be a ringed space. A **sheaf of $\mathcal{O}_X$-modules** (or, simply, an $\mathcal{O}_X$-module) is a sheaf $\mathcal{F}$ on X, such that, for every open $U \subseteq X$, $\mathcal{F}(U)$ is an $\mathcal{O}_X(U)$-module and, for every open sets $V \subseteq U$, the restriction $\mathcal{F}(U) \to \mathcal{F}(V)$ is compatible with the module structures via the ring homomorphism $\mathcal{O}_X(U) \to \mathcal{O}_X(V)$.*

A **morphism** between two $\mathcal{O}_X$-modules $\mathcal{F}$ and $\mathcal{G}$ is a morphism of sheaf such that, for each open set $U \subseteq X$, the map $\mathcal{F}(U) \to \mathcal{G}(U)$ is a morphism of $\mathcal{O}_X(U)$-modules.

The category of $\mathcal{O}_X$-modules is closed under kernel, image, cokernel, direct sum, direct or inverse limit and quotient. We can also define the tensor product of two $\mathcal{O}_X$-modules $\mathcal{F}$ and $\mathcal{G}$ in the following way: $\mathcal{F} \otimes \mathcal{G}$ is the sheaf associated to the presheaf given by $U \mapsto \mathcal{F}(U) \otimes_{\mathcal{O}_X(U)} \mathcal{G}(U)$ for every open $U \subseteq X$.

Definition 4.2 *An $\mathcal{O}_X$-module $\mathcal{F}$ is said to be **free** if it is isomorphic to the direct sum of copies of $\mathcal{O}_X$. The number of copies of $\mathcal{O}_X$ is called the **rank** of $\mathcal{F}$. $\mathcal{F}$ is **locally free** if X can be covered by open sets U such that $F_{|U}$ is a free $\mathcal{O}_X$-module.*

It can be proved that the rank of $\mathcal{O}_{X|U}$ is the same for open subsets U in the same connected component of X. Therefore, if the underlying topological space of X is connected, then it makes sense to talk about the rank of a locally free $\mathcal{O}_X$-module.

Definition 4.3 *An **invertible sheaf** on X is a locally free $\mathcal{O}_X$-module of rank 1.*

Invertible sheaves will play an important role in our work for their connections with line bundles and divisors. The next lemma explains the choice

of the word invertible and shows that the set of invertible sheaves on a ring space, endowed with the operation $\otimes$, is a group.

Lemma 4.1 *If $\mathcal{L}$ and $\mathcal{M}$ are invertible sheaves on a ringed space X, then $\mathcal{L} \otimes \mathcal{M}$ is an invertible sheaf on X and, for every invertible sheaf $\mathcal{L}$, there exists an invertible sheaf $\mathcal{L}^{-1}$ on X such that $\mathcal{L} \otimes \mathcal{L}^{-1} \cong O_X$.*

Proof: There exists a covering $\{U_i\}$ such that $\mathcal{L}_{|U_i} \cong \mathcal{M}_{|U_i} \cong \mathcal{O}_X$. So, locally, $\mathcal{L} \otimes \mathcal{M} \cong \mathcal{O}_X \otimes_{\mathcal{O}_X} \mathcal{O}_X \cong \mathcal{O}_X$. For the second part, take $\mathcal{L}^{-1} = \mathrm{Hom}(\mathcal{L}, \mathcal{O}_X)$. We get $\mathcal{L}^{-1} \otimes \mathcal{L} = \mathrm{Hom}(\mathcal{L}, \mathcal{O}_X) \otimes \mathcal{L} \cong \mathrm{Hom}(\mathcal{L}, \mathcal{L}) \cong \mathcal{O}_X$. $\square$

Definition 4.4 *The group of isomorphism classes of invertible sheaves is called the **Picard group** and denoted by $Pic(X)$.*

Let $f : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ be a morphism of ringed spaces. If $\mathcal{F}$ is an $\mathcal{O}_X$-module, then $f_*\mathcal{F}$ is an $f_*\mathcal{O}_X$-module (in fact for every $V \subseteq Y$, $\mathcal{F}(f^{-1}(V))$ is an $\mathcal{O}_X(f^{-1}(V))$-module). But we have the morphism of sheaves $f^{\#} : \mathcal{O}_Y \to f_*\mathcal{O}_X$, so $f_*\mathcal{F}$ can be viewed as an $\mathcal{O}_Y$-module. It is called the **direct image** of $\mathcal{F}$. Analogously, if G is an $\mathcal{O}_Y$-module we can construct its **inverse image** f^*G as follows: $f^{-1}\mathcal{G}$ is an $f^{-1}\mathcal{O}_Y$-module, but f^{-1} is the left adjoint of f_*, so $Hom_{\mathcal{O}_X}(f^{-1}\mathcal{O}_Y, \mathcal{O}_X) \cong Hom_{\mathcal{O}_Y}(\mathcal{O}_Y, f_*\mathcal{O}_X)$ and there exists a morphism of sheaves of rings on X from $f^{-1}\mathcal{O}_Y$ to $\mathcal{O}_X$. It gives the structure of $f^{-1}\mathcal{O}_Y$-module on $\mathcal{O}_X$. Tensoring with $f^{-1}\mathcal{G}$ we obtain the $\mathcal{O}_X$-module $f^{-1}\mathcal{G} \otimes_{f^{-1}\mathcal{O}_Y} \mathcal{O}_X$.

We describe now two important ways of associating sheaf of modules to modules.

Let A be a ring, M an A-module, $X = \mathrm{Spec}\, A$. The **sheaf $\tilde{M}$ associated** to M on X is constructed in the following way: for each open set $U \subseteq X$, let $\tilde{M}(U)$ be the set of functions $s : U \to \coprod_{p \in U} M_p$ such that $\forall p \in U$, $s(p) \in M_p$ and with the property that $\forall p \in U$ there exist V open in U, $m \in M$ and $f \in A$ such that $f \notin q \quad \forall q \in V$ and $s(q) = \frac{m}{f}$ in M_q. For open sets $U \subseteq V$ the restriction map is clearly defined.

Proposition 4.1 *Let A, M, X, $\tilde{M}$ as before. Then*

1. *$\tilde{M}$ is an $\mathcal{O}_X$-module.*
2. *$\forall p \in X$, $(\tilde{M})_p \cong M_p$.*
3. *$\Gamma(X, \tilde{M}) = M$.*

Proof: see [7, II 5.1].

Definition 4.5 *Let $(X, \mathcal{O}_X)$ be a ringed space. An $\mathcal{O}_X$-module $\mathcal{F}$ is called **quasi-coherent** if X can be covered by open affine subsets $U_i = \operatorname{Spec} A_i$ such that $\mathcal{F}_{|U_i} \cong \tilde{M}_i$ for some A_i-module M_i. $\mathcal{F}$ is **coherent** if each M_i can be chosen to be finitely generated.*

REMARK: The structure sheaf $\mathcal{O}_X$ is coherent. Since an invertible sheaf is locally isomorphic to $\mathcal{O}_X$, every invertible sheaf is coherent.

We now wonder how coherent and quasi coherent sheaves behave with respect to some elementary operations in the category of sheaves. The answer is given by the following proposition.

Proposition 4.2 *Let X be a scheme. The tensor product of two quasi-coherent sheaves is quasi-coherent. Kernel, Image and Cokernel of a morphism of quasi-coherent sheaves are quasi-coherent. Moreover, if X is locally noetherian, then the previous properties hold for coherent sheaves.*

Proof: see [15, 5.1.12]

Analogously, we can see, under suitable conditions, that direct and inverse images of (quasi-)coherent sheaves are (quasi-)coherent.

Proposition 4.3 *Let $f : X \to Y$ be a morphism of schemes.*

1. *If $\mathcal{G}$ is a quasi-coherent sheaf of $\mathcal{O}_Y$-modules, then $f^*\mathcal{G}$ is a quasi-coherent sheaf of $\mathcal{O}_X$-modules.*
2. *If X and Y are noetherian, and $\mathcal{G}$ is coherent, then $f^*\mathcal{G}$ is coherent.*
3. *Suppose X is noetherian or f is quasi-compact and separated. Then if $\mathcal{F}$ is a quasi-coherent sheaf of $\mathcal{O}_X$-modules, $f_*\mathcal{F}$ is a quasi-coherent $\mathcal{O}_Y$-module.*

Proof: see [7, II 5.8]

If $i : Y \to X$ is a closed immersion we can define the **sheaf ideal** $\mathcal{I}_Y$ associated to X in Y as the kernel of the morphism $i^{\#} : \mathcal{O}_X \to i_*\mathcal{O}_Y$.

Proposition 4.4 *Let $\mathcal{I}_Y$ be a sheaf ideal associated to a scheme Y in X. Then $\mathcal{I}_Y$ is quasi-coherent. If X is noetherian, then $\mathcal{I}_Y$ is coherent.*

Proof: A closed immersion is quasi-compact and separated, so, by proposition 4.3(3), $i_*\mathcal{O}_Y$ is quasi-coherent on X. $\mathcal{I}_Y$ is the kernel of a morphism of quasi-coherent sheaves, so it quasi coherent. Suppose X is noetherian. Locally, for every open subset $U = \operatorname{Spec} A$ of X, A is noetherian, so the ideal $I = \Gamma(U, \mathcal{I}_{Y|U})$ is finitely generated, so I_Y is coherent. □

The second construction is a projective version of the previous one. Let S be a graded ring, $X = \operatorname{Proj} S$ and M a graded S-module. For any open subset $U \subseteq \operatorname{Proj} S$, let $\widetilde{M}(U)$ be the set of functions s from U to $\coprod_{p \in U} M_{(p)}$ such that $\forall p \in U$, $s(p) \in M_{(p)}$ and for every $p \in U$, there exist V open neighborhood of p in U, $m \in M$ and $f \in S$ of the same degree with $f \notin q$ and $s(q) = \frac{m}{f}$ in $M_{(q)}$ for every $q \in V$. For two open sets $V \subseteq U$, the restriction map $\widetilde{M}(U) \to \widetilde{M}(V)$ is defined in the obvious way.

Proposition 4.5 *Let S, M, $\widetilde{M}$ as above, $X = \operatorname{Proj} S$. Then*

1. *For every $p \in X$, $(\widetilde{M})_p = M_{(p)}$.*
2. *$\widetilde{M}$ is a quasi-coherent $\mathcal{O}_X$-module. If M is finitely generated over a noetherian ring S then $\widetilde{M}$ is coherent.*

Proof: see [7, II 5.11].

We will often deal with the so-called **twisted sheaves**. Let S be a graded ring, $X = \operatorname{Proj} S$. For any $n \in \mathbf{Z}$, $S(n)$ is the graded S-module $\bigoplus S(n)_d$, where $S(n)_d = S_{n+d}$. Define $\mathcal{O}_X(n)$ as $\widetilde{S(n)}$. For any sheaf of $\mathcal{O}_X$-modules $\mathcal{F}$, the sheaf $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{O}_X(n)$ is indicated with $\mathcal{F}(n)$ and called **twisted sheaf**.

Some of the properties of twisted sheaves are shown below. We remark that, for a graded ring (or algebra, or module) S, we indicate with S_i the homogeneous degree i part of S.

Proposition 4.6 *Let S be a graded ring generated by S_1 as S_0-algebra, $X = \operatorname{Proj} S$.*

1. *The sheaf $\mathcal{O}_X(n)$ is an invertible sheaf on X.*
2. *For any graded S-module M, $\widetilde{M}(n) \cong \widetilde{M(n)}$. In particular $\mathcal{O}_X(n) \otimes \mathcal{O}_X(m) \cong \mathcal{O}_X(n+m)$.*
3. *Let T be another graded ring, generated by T_1 as a T_0-algebra, let $\varphi : S \to T$ be an homomorphism preserving degrees, $Y = \operatorname{Proj} T$, and let f be the canonical morphism from $U = \{p \in Y \mid p \not\subseteq \varphi(S_+)\}$ to X induced by φ. Then $f^*(\mathcal{O}_X(n)) \cong \mathcal{O}_Y(n)_{|U}$.*

Proof: see [7, II 5.12].

We define now the twisted sheaf $\mathcal{O}(1)$ on $\mathbb{P}^r_Y$, where Y is a scheme and $\mathbb{P}^r_Y = \operatorname{Proj} Z[x_0, \cdots, x_r]$.

Definition 4.6 *Let Y be a scheme. The **twisted sheaf** $\mathcal{O}(1)$ on $\mathbb{P}^r_Y$ is defined as $g^*(\mathcal{O}(1))$, where g is the canonical morphism from $\mathbb{P}^r_Y$ to $\mathbb{P}^r_{\mathbb{Z}} = \operatorname{Proj} \mathbb{Z}[x_0, \cdots, x_r]$.*

REMARK: If $Y = \operatorname{Spec} A$ then this definition leads to the same object $\mathcal{O}(1)$ defined on $\operatorname{Proj} A[x_0, \cdots, x_r]$. Indeed in this case $\mathbb{P}^r_Y = \operatorname{Proj} A[x_0, \cdots, x_r]$. We can in fact apply the case (3) of Proposition 4.6 to $S = \mathbb{Z}[x_0, \cdots, x_r]$, $T = A[x_0, \cdots, x_r]$, φ the canonical map from S to T, $X = \mathbb{P}^r_{\mathbb{Z}}$ and $Y = U = \mathbb{P}^r_A$.

Twisted sheaves are fundamental in our application. Indeed it can be proved that, if X is projective over a noetherian ring (hence, over a field) and $\mathcal{F}$ is a coherent sheaf over X, then $\mathcal{F}$ can be written as a quotient of a direct sum of $\mathcal{O}(n_i)$.

4.2 Divisors

In the second chapter we defined divisors on curves. Now we generalize this concept for varieties and we show the connection with invertible sheaves.

Definition 4.7 *Let X be a noetherian integral separated scheme such that every local ring $\mathcal{O}_x$ of X of dimension 1 is regular. A **prime divisor** on X is a closed integral subscheme Y of codimension 1. The free abelian group generated by the prime divisors on X is called the group of **(Weil) divisors** on X and denoted by $Div(X)$. A divisor $D = \sum n_i D_i$ is called **effective** if $n_i \geq 0$ for every n_i.*

REMARK: Equivalently, we can define prime divisors as closed irreducible subsets of codimension 1. Recalling that for every closed subset Y of X there is a unique structure such that Y is a reduced subscheme of X, the notion of prime divisor is equivalent to the of 1-cycle one.

REMARK: For our future purposes we will use normal varieties and non-singular surfaces over a field K. Both these schemes satisfy the conditions of the previous definition. Recalling that in a normal variety local rings of closed points are normal and, hence, regular, we get that local rings of points are regular. Moreover, in a variety X over an algebraically closed field, X is regular at a point x if and only if it is non-singular at x.

Now we generalize valuation of rational functions. If Y is a prime divisor, let $\eta \in Y$ be its generic point. Then the local ring $\mathcal{O}_{\eta,Y}$ is a discrete valuation ring with quotient field $K(X)$. We can associate to it a valuation v_Y on $K(X)$. For $f \in K(X)^*$, $v_Y(f)$ is an integer called the **valuation of** f at Y. We will say that f has a **pole** of order $-r$ if $v_Y(f) = r < 0$, while f has a **zero** of multiplicity r if $v_Y(f) > 0$. We can associate a divisor (f) to a non-zero rational function f, putting $(f) = \sum v_Y(f)Y$, where Y runs over the prime divisors of X. (f) is really a divisor, since the sum is finite. The proof of this fact requires that X is noetherian, while the condition that X

is separated ensures that a prime divisor X is uniquely determined by its valuation on $K(X)$.

Definition 4.8 *A divisor D is called **principal** if $D = (f)$ for some $f \in K(X)^*$. It is called **locally principal** if X can be covered by $\{U_i\}$ such that $D_{|U_i} = (f_i)_{|U_i}$ for rational functions $f_i \in K(X)^*$.*

The map $f \to (f)$ is a group homomorphism form $(K(X)^*, \cdot)$ to $(Div(X), +)$. Taking the quotient of $Div(X)$ with this subgroup we get the group $Cl(X)$ of **divisor classes**.

Definition 4.9 *Two divisors D_1 and D_2 are called **linearly equivalent** if they are equal in $Cl(X)$. In this case we write $D_1 \approx D_2$.*

Let X be a noetherian integral separated scheme such that every local ring $\mathcal{O}_x$ of X of dimension 1 is regular and let $D \in \mathrm{Div}(X)$ be a locally principal sheaf on X. Take a covering $\{U_i\}$ such that $D_{|U_i} = (f_i)_{|U_i}$ for rational functions $f_i \in K(X)^*$. Put

$$\Gamma(U_i, \mathcal{L}(D)) = f_i^{-1}\mathcal{O}_X(U_i) \subseteq K(X).$$

We remark that $(f_j)_{|U_i \cap U_j} = D_{|U_i \cap U_j} = (f_i)_{|U_i \cap U_j}$, so $(f_i {f_j}^{-1})_{|U_i \cap U_j} = 0$. Then $f_i {f_j}^{-1} \in \mathcal{O}_X(U_i \cap U_j)$, hence f_i and f_j determine the same sub-$\mathcal{O}_X(U_i \cap U_j)$-module of $K(X)$. Thus, we can glue the modules $\Gamma(U_i, \mathcal{L}(D))$ to obtain a sheaf of $\mathcal{O}_X$-module $\mathcal{L}(D)$, independent by the choice of the covering $\{U_i\}$ and functions f_i.

Proposition 4.7 *Let X be a noetherian integral separated scheme such that every local ring $\mathcal{O}_x$ of X of dimension 1 is regular.*

1. *For every locally principal divisor D, the sheaf $\mathcal{L}(D)$ is invertible. The map $D \mapsto \mathcal{L}(D)$ gives a 1-1 correspondence between locally principal divisors and invertible subsheaves of the constant sheaf $K(X)$.*
2. *$\mathcal{L}(D_1 - D_2) \cong \mathcal{L}(D_1) \otimes \mathcal{L}(D_2)^{-1}$.*
3. *$D_1 \approx D_2$ if and only if $\mathcal{L}(D_1) \cong \mathcal{L}(D_2)$ as invertible sheaves.*

Proof:

1. Let $\{U_i\}$ be an open covering of X such that $D_{|U_i} = (f_i)_{|U_i}$. The map $\mathcal{O}_X(U_i) \to \Gamma(U_i, L(D))$ sending 1 to ${f_i}^{-1}$ is an isomorphism, so $\mathcal{L}(D)_{|U_i} = O_{U_i}$. Given an invertible subsheaf of $K(X)$, take a covering $\{V_i\}$ such that $\mathcal{L}_{|V_i} \cong \mathcal{O}_{V_i}$. Let $g_i \in K(X)^*$ be the inverse of the generator of $\mathcal{L}_{|V_i}$. From the collection $\{V_i, g_i\}$ we construct a divisor D in the following way: for each prime divisor Y, take the coefficient of

Y to be $v_Y(g_i)$, where $Y \cap V_j \neq \emptyset$. The coefficient of Y is well-defined; in fact in the case $V_j \cap Y \neq \emptyset$, then $g_i {g_j}^{-1}$ is invertible in $U_i \cap U_j$, so $v_Y(g_i {g_j}^{-1}) = 0$ and $v_Y(g_i) = v_Y(g_j)$. It is clear that this construction defines the inverse of the map $D \mapsto \mathcal{L}(D)$.

2. Take a covering $\{U_i\}$ such that $D_{1|U_i} = (f_i)_{|U_i}$ and $D_{2|U_i} = (g_i)_{|U_i}$. Then, on U_i, $D_1 - D_2 = (f_i g_i^{-1})$. The subsheaf of $K(X)$ corresponding to $\{U_i, f_i {g_i}^{-1}\}$ is $\mathcal{L}(D_1)\mathcal{L}(D_2)^{-1}$, which is isomorphic to the invertible sheaf of $\mathcal{O}_X$-module $\mathcal{L}(D_1) \otimes \mathcal{L}(D_2)^{-1}$.

3. First we show that D is principal if and only if $\mathcal{L}(D) \cong O_X$. If D is principal then $D = (f)$ for some $f \in K(X)^*$ and $L(D)$ is defined by the covering (X, f^{-1}), so sending $1 \mapsto f^{-1}$ gives an isomorphism $\mathcal{O}_X \cong \mathcal{L}(D)$.
On the contrary, given an isomorphism $\mathcal{L}(D) \cong \mathcal{O}_X$, the image of $1 \in \mathcal{O}_X(X)$ is an element of $\Gamma(X, K(X)^*)$ whose inverse defines D as principal divisor. Now apply this result and point (2) to $D = D_1 - D_2$. We have $D_1 = D_2$ in $Cl(X) \iff D_1 - D_2$ is principal $\iff \mathcal{L}(D_1 - D_2) = \mathcal{L}(D_1) \otimes \mathcal{L}(D_2)^{-1} \cong \mathcal{O}_X \iff \mathcal{L}(D_2) \cong \mathcal{L}(D_2)$.

Corollary 4.1 *Let X be as before. The map $D \to \mathcal{L}(D)$ induces an isomorphism between the group equivalence classes of locally principal divisor and $Pic(X)$.*

Proof: We just have to show that every invertible sheaf $\mathcal{L}$ on X is isomorphic to a subsheaf of $K(X)$. Now take $\mathcal{L} \otimes_{\mathcal{O}_X} K(X)$. On every open set U where $\mathcal{L} \cong \mathcal{O}_X$, we have $\mathcal{L} \otimes_{\mathcal{O}_X} K(X) \cong K(X)$. $\mathcal{L} \otimes_{\mathcal{O}_X} K(X)$, restricted to each open of a covering, is constant and so it is constant, as X is integral, hence irreducible. The map $\mathcal{L} \to \mathcal{L} \otimes_{\mathcal{O}_X} K(X)$ expresses $\mathcal{L}$ as a subsheaf of $K(X)$. □

Lemma 4.2 *Let X be an integral, separated, noetherian scheme, all of whose local rings are unique factorization domains. Then every divisor on X is locally principal.*

Proof: see [7, II 6.11 and 6.11.2]

Corollary 4.2 *If X is a smooth variety over then $Cl(X) \cong Pic(X)$, via the map induced by $D \mapsto \mathcal{L}(D)$.*

Let $\mathcal{L}$ be an invertible sheaf on a nonsingular projective variety over an algebraically close field K. By what we said above we know that $\mathcal{L} \cong \mathcal{L}(D)$ for a divisor D, and $\mathcal{L}$ is isomorphic to a a subsheaf of $K(X)$. We can associate to every nonzero global section $s \in \Gamma(X, \mathcal{L}(D))$ the divisor $Z(s)$, by putting $Z(s) = (s) + D$. $Z(s)$ is called the **divisor of zeros** of s. If D is a

divisor on X we denote by $|D|$ the set of effective divisors linearly equivalent to D. It is very easy, by looking at the definitions and the previous proofs, to prove the following proposition.

Proposition 4.8 *Let D be a divisor on a variety X, defined over an algebraically closed field K. Then the map*

$$\Gamma(X, \mathcal{L}(D)) \setminus \{0\} \longrightarrow |D|$$

$$s \longmapsto Z(s)$$

induces a bijection between $|D|$ and $\Gamma(X, \mathcal{L}(D)) \setminus \{0\}/K^*$.

4.3 Definition of AG codes on varieties

In this paragraph we define an algebraic geometric code over a variety, as in [21].

Lemma 4.3 *Let K be a field, X a projective scheme over K, $\mathcal{L}$ an invertible sheaf on X. Then $\Gamma(X, \mathcal{L})$ is a finite-dimensional K-vector space.*

Proof: It comes from [7, II 5.19] and the remark at page 43.

For a scheme X over $\mathbf{F}_q$, an invertible sheaf $\mathcal{L}$ and an $\mathbf{F}_q$-rational point $P \in X$, call $\mathcal{L}_P/m_P\mathcal{L}_p$ the **fiber** of $\mathcal{L}$ at P and indicate it with $\overline{\mathcal{L}}_P$. Since $\mathcal{L}$ is locally isomorphic to $\mathcal{O}_X$, $\overline{\mathcal{L}}_P \cong \mathcal{O}_P/m_p\mathcal{O}_P = \mathbf{F}_q$. Chosen a **trivialization** at $\overline{\mathcal{L}}_P$, i.e. an isomorphism φ between $\overline{\mathcal{L}}_P$ and $\mathbf{F}_q$, the **value of** $s \in \Gamma(X, \mathcal{L})$ **at** P is $\varphi(s_p + m_p\mathcal{L}_p) \in \mathbf{F}_q$.

Definition 4.10 *Let X be a projective scheme over $\mathbf{F}_q$, $\mathcal{L}$ an invertible sheaf, $\mathcal{P} = \{P_1, \cdots, P_n\}$ a set of $\mathbf{F}_q$-rational points. Chosen for every every P_i a trivialization at $\overline{\mathcal{L}}_{P_i}$, we have the germ map*

$$\alpha : \Gamma(X, \mathcal{L}) \longrightarrow \mathbf{F}_q^n$$

$$s \longmapsto (s_1, \cdots, s_n)$$

where s_i is the value of s at P_i. The code $C(X, \mathcal{P}, \mathcal{L})$ is defined as the image of α.

REMARKS:

- If X is a smooth projective variety and $\mathcal{L} = \mathcal{L}(G)$ for some $G \in Div(X)$, then $\Gamma(X, \mathcal{L}) = L(G)$, where $L(G) = \{f \in K(X)^* \mid (f) + G \text{ is effective}\} \cup \{0\}$. Thus, for smooth projective curves, we find again the classical AG codes. Moreover, take $s \in \Gamma(X, L(G)) \setminus \{0\}$ and $P \in C$, where C is a prime divisor on X. Then the value of s at P is 0 if and only if the divisor of zeros $Z(s)$ contains C.

- We see that different trivializations produce different codes, but all these codes are equivalent (in the sense of definition 2.3), so different trivializations produce codes with the same parameters.

NOTE: [21] uses the word *line bundle* instead of *invertible sheaf*. Exercise II 5.18 in [7] defines line bundles and shows that there is a one-to-one correspondence between the Picard group and isomorphism classes of line bundles. We just remark that, under this correspondence, a section of a line bundle is a global section of the invertible sheaf, so the terminology is good and no confusion results.

5 Codes on surfaces

Even if Tsfasman and Vladut's definition of AG codes on a variety is not so recent ([22](1982)), the first deep work about a class of codes on higher dimensional varieties is due to the danish mathematician Hansen, who studied in his PhD thesis codes on surfaces and Deligne-Lusztig varieties ([6](2001)). Another work about codes on surfaces, independent by Hansen's results, is by Voloch and Zarzar ([27]).

As usual, the geometry background is introduced in the first subsections.

5.1 Ample and very ample invertible sheaves

Definition 5.1 *Let X be a scheme over Y. An invertible sheaf $\mathcal{L}$ is said to be **very ample** if there exists a immersion $i : X \to \mathbb{P}^r_Y$ for some r such that $\mathcal{L} \cong i^*(\mathcal{O}(1))$.*

Definition 5.2 *Let X be a scheme, and let $\mathcal{F}$ be a sheaf of $\mathcal{O}_X$-modules. We say that $\mathcal{F}$ is **generated by global sections** if there are global sections $\{s_i\}_{i\in I}$ of $\mathcal{F}$ such that, for every $x \in X$, the images of s_i in the stalk $\mathcal{F}_x$ generate the stalk as $\mathcal{O}_x$-module.*

EXAMPLE: Take a ring A, and a coherent sheaf $\mathcal{F} = \tilde{M}$ on $\operatorname{Spec} A$, where M is an A-module. $\mathcal{F}$ is generated by every set of generators of M as A-module. Indeed we know that for every $p \in \operatorname{Spec} A$, $\tilde{M}_p = M_p$.

EXAMPLE: Let $X = \operatorname{Proj} S$, where S is a graded ring generated by S_1 as S_0-algebra and let $\mathcal{F} = \mathcal{O}_X(1)$. For every $p \in \operatorname{Proj} S$, $\mathcal{O}_{X,p} \cong S_{(p)}$ and $\mathcal{F}_p \cong S(1)_{(p)}$. Therefore it is clear that the elements of S_1 give global sections that generate $\mathcal{O}_X(1)$.

EXAMPLE: Let A be a ring, $X = \operatorname{Proj} A[x_0, \cdots, x_r]$. Then $x_0, \cdots, x_r$ are global sections of $\mathcal{O}_X(1)$ which generate it.

EXAMPLE: If A is a ring and $\varphi : X \to \mathbb{P}^r_A$ is an A-morphism, then the $\mathcal{O}_X$-sheaf $\varphi^*(\mathcal{O}_X(1))$ is generated by the global sections $s_0, \cdots, s_r$, where $s_i = \varphi^*(x_i)$.

Definition 5.3 *An invertible sheaf $\mathcal{L}$ on a noetherian scheme X is said to be **ample** if for every coherent $\mathcal{O}_X$-sheaf there is an integer $n_0 > 0$ such that, for every $n \geq n_0$, $\mathcal{F} \otimes \mathcal{L}^n$ is generated by global sections.*

Definition 5.4 *Let X be a nonsingular variety. Then a divisor D is said to be **ample** (resp. **very ample**) if the corresponding invertible sheaf $\mathcal{L}(D)$ is ample (resp. very ample).*

The propositions below shows the relation between ample and very ample invertible sheaves under suitable conditions and, in particular, in the case of varieties.

Proposition 5.1 *Let X be a scheme of finite type over a noetherian ring A, and let $\mathcal{L}$ be an invertible sheaf. Then L is ample if and only if $\mathcal{L}^m$ is very ample over* $\operatorname{Spec} A$ *for some $m > 0$.*

EXAMPLE: Let D be a divisor on a projective nonsingular curve X and $\mathcal{L} = \mathcal{L}(D)$. It can be proved, as consequence of the Riemann-Roch theorem, that $\mathcal{L}$ is ample if and only if $\deg D > 0$.

EXAMPLE: Let $X = \mathbb{P}^n_K$, where K is a field. $\mathcal{O}(1)$ is very ample by definition. Let $d > 0$. Put $S = K[x_0, \cdots, x_n]$ and consider the graded K-algebra $S^{(d)} = \bigoplus S_n^{(d)}$, where $S_n^{(d)} = S_{nd}$. The map $\varphi : S \to S^{(d)}$ which sends x_i to x_i^d preserves the grading and induces an isomorphism between $\operatorname{Proj} S$ and $\operatorname{Proj} S^{(d)}$. Under this isomorphism the sheaf $\mathcal{O}_X(d)$ on $\mathbb{P}^n_K$ corresponds to the invertible sheaf $\mathcal{O}(1)$ on $\operatorname{Proj} S^{(d)}$, so $\mathcal{O}_X(d)$ is very ample, hence ample. If $d < 0$ then $\mathcal{O}(d)$ has non global sections, so it is not ample and not very ample. We conclude that $\mathcal{O}(d)$ is ample if and only if it is very ample if and only if $d > 0$.

Lemma 5.1 *Let X be a scheme of finite type over a noetherian ring. If $\mathcal{L}$ is a very ample invertible sheaf and $\mathcal{M}$ is an invertible sheaf generated by global sections, then $\mathcal{L} \otimes \mathcal{M}$ is very ample.*

Corollary 5.1 *Let X be as in the previous lemma and let $\mathcal{L}$ be an ample invertible sheaf. Then, for every invertible sheaf $\mathcal{M}$ on X, there exists $n > 0$ such that $\mathcal{M} \otimes \mathcal{L}^n$ is very ample.*

Proof: $\mathcal{L}$ is ample and $\mathcal{M}$ coherent, so there exists $k > 0$ such that $\mathcal{M} \otimes \mathcal{L}^n$ is generated by global sections. Moreover, there exists $l > 0$ such that $\mathcal{L}^l$ is very ample. Thus $\mathcal{M} \otimes \mathcal{L}^{kl} = (\mathcal{M} \otimes \mathcal{L}^n) \otimes \mathcal{L}^l$ is very ample by previous lemma. □

We will treat later the case of ample and very ample invertible sheaves on surfaces.

5.2 Arithmetic and geometric genus of varieties

We suppose the basic notions of homological algebra and theory of categories to be know and we focus on our case, namely the category $\mathbf{Mod}(\mathbf{X})$ of sheaves of $\mathcal{O}_X$-modules on a ringed space $(X, \mathcal{O}_X)$. First let us remark that $\mathbf{Mod}(\mathbf{X})$ is an abelian category with enough injectives. This comes from the well-known fact that every module sits inside an injective one.

Definition 5.5 *Let $(X, \mathcal{O}_X)$ be a ringed space and let $\Gamma(X, \cdot)$ be considered as functor from* $\mathbf{Mod}(\mathbf{X})$ *to the category* **Ab** *of abelian groups. For any $\mathcal{O}_X$-sheaf $\mathcal{F}$, the i-th* ***cohomology functor*** *$H^i(X, \cdot)$ is defined as the i-th right derived functor of $\Gamma(X, \cdot)$. For any $\mathcal{O}_X$-sheaf $\mathcal{F}$, the group $H^i(X, \mathcal{F})$ is called the i-th* ***cohomology group*** *of $\mathcal{F}$.*

REMARK: For every $\mathcal{O}_X$-sheaf $\mathcal{F}$, $H^0(X, \mathcal{F}) = \Gamma(X, \mathcal{F})$ is a $\Gamma(X, \mathcal{O}_X)$-module, so all the $H^i(X, \mathcal{F})$ have a structure of $\Gamma(X, \mathcal{O}_X)$-module. The dimension of the i-th group of cohomology is indicated with h^i. Moreover we know that if X is a projective variety over an algebraically closed field K, then $\Gamma(X, \mathcal{O}_X) \cong K$.

The two following theorems are necessary to introduce the arithmetic genus of a projective variety. [7] states the first one for sheaves of abelian group on a noetherian topological space. Our choice is due to our definition of cohomology functor. Remark that Lemma 4.3 at page 48 is a particular case of the second theorem.

Theorem 5.1 (Grothendieck) *Let $(X, \mathcal{O}_X)$ be a noetherian ringed topological space of dimension n. Then, for all $i > n$ and all sheaves of $\mathcal{O}_X$-modules $\mathcal{F}$, we have $H^i(X, \mathcal{F}) = 0$.*

Theorem 5.2 (Serre) *Let X be a projective scheme over a noetherian ring A, and let $\mathcal{O}_X(1)$ be a very ample invertible sheaf on X over* $\operatorname{Spec} A$. *Let $\mathcal{F}$ be a coherent sheaf on X. Then for each $i \geq 0$, $H^i(X, \mathcal{F})$ is a finitely generated A-module.*

Definition 5.6 *Let X be a projective scheme of dimension r over a field K. Then the* ***arithmetic genus*** *is*

$$p_a(X) = (-1)^r(\chi(O_X) - 1),$$

where $\chi(O_X) = \sum(-1)^i h^i(X, \mathcal{O}_X)$.

Lemma 5.2 *If X is a projective variety of dimension r over an algebraically closed field K, then $p_a(X) = \sum_{i=0}^{r-1}(-1)^i \dim_K H^{r-i}(X, \mathcal{O}_X)$.*

Proof: As already observed, $H^0(X, \mathcal{O}_X) \cong K$, so $h^0(X, \mathcal{O}_X) = 1$ and, by Grothendieck's theorem, $h^i(X, \mathcal{O}_X) = 0$ for $i > r$. Thus $p_a(X) = (-1)^r \sum_{i=1}^{r}(-1)^i h^i(X, \mathcal{O}_X) = \sum_{i=0}^{r-1}(-1)^i h^{r-i}(X, \mathcal{O}_X)$. □

We briefly introduce now the sheaf of differentials, just in order to define the geometric genus of a projective variety. We will see later the properties of sheaves of differentials are strictly related to those of Kähler differentials, and so we suggest as reference for the latter topic any good book in commutative algebra, e.g. [14].

Let X be a scheme over Y. The diagonal map $\Delta : X \to X \times_Y X$ induces an isomorphism between X and its image $\Delta(X)$. Moreover $\Delta(X)$ is a closed subscheme of an open subscheme W of $X \times_Y X$. So we can consider the ideal sheaf $\mathcal{I}$ associated to $\Delta(X)$ in W.

Definition 5.7 *The **sheaf of relative differentials** of X over Y is the sheaf $\Gamma_{X/Y} = \Delta^*(\mathcal{I}/\mathcal{I}^2)$.*

Lemma 5.3 *Let X be a scheme over Y. Then $\Omega_{X/Y}$ is a quasi-coherent $\mathcal{O}_Y$-module. If Y is noetherian and X of finite type over Y, then $\Omega_{X/Y}$ is coherent.*

Proof: $\mathcal{I}/\mathcal{I}^2$ has a structure of $\mathcal{O}_{\Delta(X)}$-module, but Δ is an isomorphism between X and $\Delta(X)$, so $\Delta^*(\mathcal{I}/\mathcal{I}^2) = \Omega_{X/Y}$ has a structure of $\mathcal{O}_X$-module. $\mathcal{I}/\mathcal{I}^2$ is quasi-coherent by Proposition 4.2, hence $\Delta^*(\mathcal{I}/\mathcal{I}^2)$ is quasi coherent by proposition 4.3. If Y is noetherian and X of finite type, then $X \times_Y X$ is noetherian, so $\mathcal{I}/\mathcal{I}^2$ is coherent. Using Proposition 4.3 we have that $\Omega_{X/Y}$ is coherent. □

EXAMPLE: Take $X = \operatorname{Spec} B$, $Y = \operatorname{Spec} A$ and $f : X \to Y$. In this case, $X \times_Y X = \operatorname{Spec} B \otimes_A B$ and Δ is induced by the morphism $\varphi : B \otimes_A B \to B$ which sends $b_1 \otimes b_2$ to $b_1 b_2$. If I is the kernel of φ, we have $\mathcal{I}/\mathcal{I}^2 = \widetilde{(I/I^2)}$. Thus $\Omega_{X/Y}$ is the sheaf associated to $\Omega_{B/A}$, where $\Omega_{B/A}$ is the module of relative differential forms of B over A.

Definition 5.8 *Let X be a nonsingular variety of dimension n over a field K. The **canonical sheaf** of X is $\omega_X = \Lambda^n \Omega_{X/K}$, i.e. the n-th exterior power of the sheaf of differentials of X over K.*

REMARK: If X is a nonsingular variety of dimension n over an algebraically closed field K, then it is not hard to prove, by using results from theory of Kähler differentials, that $\Omega(X/Y)$ is a locally free $\mathcal{O}_X$-module of rank n. Therefore ω_X is an invertible sheaf.

Proposition 5.2 *Let Y be a nonsingular irreducible curve on a nonsingular variety X. Then $\omega_Y = \omega_X \otimes \mathcal{L}(Y) \otimes \mathcal{O}_Y$.*

Proof: see [7, II 8.20]

Definition 5.9 *If X is a nonsingular variety of dimension n over an algebraically closed field K the the **geometric genus** of X is the nonnegative integer $p_g = \dim_K \Gamma(X, \omega_X)$.*

IMPORTANT REMARK: Alternatively, using cohomology, we could define p_g as the dimension of the n-th cohomology group of $\mathcal{O}_X$. The equivalence of the two definitions follows from the Serre duality theorem. By Serre duality theorem, in fact, we have also that, if D is a divisor over a nonsingular variety X of dimension n, then $h^0(X, \mathcal{L}(W - D)) = h^n(X, \mathcal{L}(D))$, where W is a canonical divisor on X.

EXAMPLE: For a nonsingular projective curve X over K algebraically closed, $p_a = h^1(X, \mathcal{O}_X) = \dim \Gamma(X, \omega_X) = g$. In particular we can write the invertible sheaf ω_X as $\mathcal{L}(W)$, where W is a canonical divisor. We find $g := p_g = p_a = \dim \Gamma(X, \mathcal{L}(W)) = \dim L(W)$.

EXAMPLE: For a nonsingular projective surface X over an algebraically closed field K, we get $p_a = h^2(X, \mathcal{O}_X) - h^1(X, \mathcal{O}_X)$, while $p_g = h^2(X, \mathcal{O}_X)$. The geometric genus is therefore larger than the arithmetic genus and the difference $h^1(X, \mathcal{O}_X)$ is called the **irregularity** of X.

5.3 Basic properties of surfaces

In the following, with the word *surface* we will mean a nonsingular projective surface over an algebraically closed field K. A curve is an effective divisor on the surface and a point is a closed point.

The first step is defining the intersection between divisors on a surface. For the proofs we refer to [7, V 1].

Definition 5.10 *If C and D are curves on X passing through a point $P \in X$, we indicate with $(C.D)_P$ the integer $\dim(f, g)/m_P$, where f and g are local equations for C and D respectively and m_P is the maximal ideal of $\mathcal{O}_{P,X}$. We say that C and D **meet transversally** if $(C.D)_P = 1$.*

We would like to define the intersection number $C.D$ between divisors C and D such that the following natural properties hold for every $C, D, E \in \mathrm{Div}(X)$.

1. If C and D are nonsingular curves meeting transversally, then $C.D = \#(C \cap D)$.
2. The intersection number is symmetric, i.e. $C.D = D.C$.
3. The intersection number is additive, i.e. $C + E.D = C.D + E.D$.
4. It depends only on the linear equivalence classes.

Theorem 5.3 *There is a unique pairing $Div(X) \times Div(X) \to \mathbb{Z}$, which sends (C, D) to $C.D$, such that properties 1-4 hold.*

We state an auxiliary lemma for the proof of this theorem, because we will use it in the following.

Lemma 5.4 *Let C be an irreducible nonsingular curve over a surface X and let D be any curve meeting C transversally. Then*

$$\#(C \cap D) = \deg_C(\mathcal{L}(D) \otimes \mathcal{O}_C),$$

where $\deg_C(\mathcal{L}(D) \otimes \mathcal{O}_C)$ is the degree of the divisor on C corresponding to the invertible sheaf $\mathcal{L}(D) \otimes \mathcal{O}_C$.

The following proposition gives an explicit way to calculate the intersection number in a particular case.

Proposition 5.3 *If C and D are curves on X having no common irreducible component, then*

$$C.D = \sum_{P \in C \cap D} (C.D)_P.$$

The next theorem gives an important connection between the genus of a nonsingular curve on a surface and the intersection number.

Proposition 5.4 (adjunction formula) *If C is a nonsingular curve of genus g on the surface X and W is the canonical divisor on X, then*

$$2g - 2 = C.(C + W).$$

Proof: By Proposition 5.2, $\omega_C = \omega_X \otimes \mathcal{L}(C) \otimes \mathcal{O}_C$. We know that the degree of a canonical sheaf on a smooth curve is $2g - 2$. On the other hand, $\deg_C(\omega_C \otimes \mathcal{L}(C) \otimes \mathcal{O}_C) = \deg_C(\mathcal{L}(C + W) \otimes O_C) = C.(C + W)$ by Lemma 5.4 and the properties of the intersection number. □

We state now the Riemann-Roch theorem for surfaces. For a divisor D on a surface X, we let $l(D) = h^0(X, \mathcal{L}(D))$.

Theorem 5.4 (Riemann-Roch) *If D is any divisor on the surface X of arithmetic genus p_a and W is a canonical divisor, then*

$$l(D) - h^1(X, L(D)) + l(W - D) = \frac{1}{2}D.(D - W) + 1 + p_a \ .$$

We want to emphasize that the Riemann-Roch theorem is fundamental for our problem of calculating the parameters of codes over surfaces. Indeed, inserting conditions for the injectivity of the germ map α at page 48, $l(D)$ is the dimension of our code.

We introduced very ample and ample divisors in subsection 5.1. Now we explain why these classes of divisors are so important in the case of surfaces. In particular the next theorem gives a criterion to recognize ample divisors, while the following results are consequences of the necessity of that criterion.

Theorem 5.5 (Nakai-Maishezon criterion) *A divisor D on the surface X is ample if and only if $D.D > 0$ and $D.C > 0$ for all the irreducible curves C in X.*

Lemma 5.5 *Let H be an ample divisor on the surface X. Then there is an integer n_0 such that, if $D.H > n_0$, then $h^2(X, \mathcal{L}(D)) = 0$.*

Proof: We can take $n_0 = W.H$. By contradiction, assume $D.H > W.H$ and $h^2(X, \mathcal{L}(D)) > 0$. Recalling that $h^2(X, \mathcal{L}(D)) = l(W - D)$, the condition $h^2(X, \mathcal{L}(D)) > 0$ implies that there exists an effective divisor D', linearly equivalent to $W - D$. Write $D' = \sum_i m_i D_i$, where $m_i > 0$ and D_i are irreducible curves. We have $(W - D).H = D'.H = \sum_i m_i D_i.H > 0$ by the Nakai-Maishezon criterion. So $W.H > D.H$, which is a contradiction. □

Corollary 5.2 *Let H be an ample divisor on X and let D be a divisor such that $D.H > 0$ and $D.D > 0$. Then for a sufficiently large positive integer n, nD is linearly equivalent to an effective divisor.*

Proof: We can apply the Riemann-Roch theorem to nD, with $n > 0$. We get $l(nD) + h^2(X, nD) - h^1(X, nD) = \frac{1}{2}n^2 D.D - \frac{1}{2}nD.H + 1 + p_a$. We have $n > 0$, $D.D > 0$, $D.H > 0$ and $h^2(X, nD) = 0$ for $n > n_0$. So $l(nD) \geq h^2(X, nD) + \frac{1}{2}n^2 D.D - \frac{1}{2}nD.H + 1 + p_a$. Therefore $\lim_{n\to\infty} l(nD) = +\infty$. □

Definition 5.11 *A divisor D on a surface X is **numerically equivalent to 0** ($D \equiv 0$) if $D.E = 0$ for all divisors E. The group $\frac{Div(X)}{\equiv}$ is indicated by $Num(X)$ and two divisors are called **numerically equivalent** if they are equal in $Num(X)$.*

Definition 5.12 *A divisor D on a surface X is called **numerically effective** (**nef** for short) if $D.C \geq 0$ for every irreducible curve C on X.*

Clearly every ample divisor is nef.

5.4 Parameters of codes on surfaces

We present now some general results about codes on surfaces. The results come from [27] and [16] and give bounds for parameters of some codes on surfaces. Let X be a surface over $\mathbb{F}_q$, $\mathcal{P} = \{P_1, \cdots, P_n\}$ a set of $\mathbb{F}_q$-rational points and $\mathcal{L} = \mathcal{L}(G)$ the invertible sheaf associated to a divisor G. To calculate the minimal distance d of the code $C(X, P, \mathcal{L}(G))$ we have to bound the number of zeros of the germ map $\alpha : H^0(X, \mathcal{L}) \to \mathbb{F}_q^n$. The first trivial observation is that, for every $s \in H^0(X, \mathcal{L}) \setminus \{0\}$, the weight of $\alpha(s)$ is at least $n - \#Z(s)(\mathbb{F}_q)$, i.e. $\alpha(s)$ cannot have more zeros than the number of $\mathbb{F}_q$-rational points in the support of $Z(s)$. The Hasse-Weil bound at page 18

gives an upper bound for the number of $\mathbb{F}_q$-rational points of an irreducible curve. It is immediate to deduce from Theorem 2.6 an upper bound for the number of rational point of a curve.

Proposition 5.5 *A curve of arithmetic genus g and with r irreducible components defined over $\mathbb{F}_q$ has at most $r(q+1)+2g\sqrt{q}$ rational points.*

If s and s' are two nonzero global sections of $L(G)$ the $Z(s)$ and $Z(s')$ are linearly equivalent. Therefore the arithmetic genus of $Z(s)$ is the same of $Z(s')$. The only problem is how to control the number r of irreducible components.

Lemma 5.6 *Let X be a surface. If $Num(X)$ is generated by an ample divisor H and $G \equiv mH$, then, for every $s \in H^0(X, \mathcal{L}(G)) \setminus \{0\}$, $Z(s)$ has at most m irreducible components.*

Proof: If $s \in H^0(X, \mathcal{L}(G)) \setminus \{0\}$, write $Z(s) = k_1A_1 + \cdots + k_rA_r$, with $k_i > 0$ and A_i irreducible. As $Num(X)$ is generated by H we have $A_i \equiv a_iH$ for some a_i. Moreover, $a_i > 0$, since H is ample so $0 < A_i.H = a_iH.H$ and $H.H > 0$. $Z(s)$ is equivalent to G, so $rH.H \leq \sum K_ia_iH.H = Z(s).H = G.H = mH.H$. We get that $r \leq m$. □

NOTE: [27] replaces $Num(X)$ with the Neron-Severi group of X, but that is a more restrictive hypothesis.

Corollary 5.3 *Let X be a surface with $Num(X)$ generated by an ample divisor H and let $G \equiv mH$. Then the code $C(X, \mathcal{P}, \mathcal{L}(G))$ has distance $d \geq n - m(q+1) - 2g\sqrt{q}$, where g is is the arithmetic genus of a divisor of zeros.*

Lemma 5.7 *Suppose H is an ample divisor irreducible over the ground field $\mathbb{F}_q$ but decomposing on a Galois extension of prime degree p as a sum of p conjugate irreducible components $H_1, \cdots, H_p$, such that the intersection points are also moved by Galois. If $G \equiv mH$, then, for every $s \in H^0(X, \mathcal{L}(G)) \setminus \{0\}$, $Z(s)$ has at most $mH.H/p$ absolutely irreducible components over $\mathbb{F}_q$.*

Proof: Take $s \in H^0(X, \mathcal{L}(G)) \setminus \{0\}$ and write $k_1A_1 + \cdots + k_rA_r$ with $k_i > 0$ and A_i irreducible over $\mathbb{F}_q$. Then $0 < A_i.H = \sum_{j=1}^{p} A_i.H_j$, hence $A_i.H \geq p$. So $rp \leq \sum k_iA_i.H = Z(s).H.G.H = mH.H$. As $H.H > 0$, $r \leq mH.H/p$. □

Even if it could maybe be possible to obtain better bounds for the number of irreducible components of the divisors of zeros, this is not the best approach to get tight bounds for codes. In fact, fixing X and G, we gave bounds for every code $C(X, \mathcal{P}, \mathcal{L}(G))$ of length n, but we did not consider

the choice of the points of $\mathcal{P}$. Depending on the choice of $P_1, \cdots, P_n$ we can have different minimum distances. Therefore it is useful to follow the approach introduced by Hansen in [6].

Proposition 5.6 (Hansen) *Let X be a projective surface defined over $\mathbb{F}_q$. Let $C_1, \cdots, C_r$ be irreducible curves on X with $\mathbb{F}_q$-rational points $\mathcal{P} = \{P_1, \cdots, P_n\}$. Suppose for each C_i we have $\#C_i(\mathbb{F}_q) \leq N$. Let $\mathcal{L}$ be an invertible sheaf corresponding to a divisor G such that $G.C_i \geq 0$ for all i. Let*

$$l = \sup_s \#\{i : Z(s) \text{ contains } C_i\} \ .$$

Then the code $C(X, \mathcal{P}, \mathcal{L})$ has minimum distance

$$d \geq n - lN - \sum_{i=1}^{r} G.C_i \ .$$

If $G.C_i = \eta \leq N$ for every i, then $d \geq n - lN - (r-l)\eta$.

Proof: Take $s \in H^0(X, \mathcal{L}(G)) \setminus \{0\}$ and $Z(s)$ the divisor of zeros of s. The number of zero coordinates of $\alpha(s)$ is $\#(Z(s) \cap \cup_i C_i)(\mathbb{F}_q)$. We can write it as $\#(Z(s) \cap \cup_{C_i \subseteq D} C_i)(\mathbb{F}_q) + \#(Z(s) \cap \cup_{C_i \not\subseteq D} C_i)(\mathbb{F}_q)$. The last term, by Proposition 5.3, is less than $\sum_{C_i \not\subseteq D} Z(s).C_i$, while the latter is less than lN. By hypothesis, we have $\sum_{C_i \subseteq D} C_i.G \leq \sum_i C_i.G$ and so $w(\alpha(s)) \geq n - lN - \sum_i C_i.G$.
If $C_i.G = \eta \leq N$ for each curve, then the worst case occurs when $Z(s)$ contains exactly l curves. In this case $Z(s)$ has at most $lN + (r-l)\eta$ zeros. □

Corollary 5.4 *If $n > lN + \sum_{i=1}^{r} G.C_i$ then the germ map $\alpha : \Gamma(X, \mathcal{L}(G)) \to \mathbb{F}_q^n$ is injective.*

Corollary 5.5 *Assume also that X is a surface and H is a nef divisor on X with $H.C_i > 0$ for all i. Then*

$$l \leq \frac{G.H}{min_i\{C_i.H\}} \ .$$

Therefore, if $G.H < C_i.H$ for every i, then $l = 0$ and $d \geq n - \sum_{i=1}^{r} G.C_i$.

Proof: Take $s \in H^0(X, \mathcal{L}(G)) \setminus \{0\}$ such that $Z(s)$ contains l curves. It exists by construction. Hence $G.H = Z(s).H \geq \min\{C_i.H\}l$ because H is numerically effective and $Z(s)$ is effective. □

6 Codes on ruled surfaces

6.1 The projective space bundle

We focus now on codes over ruled surfaces, mainly studied by Lomont. In his PhD thesis ([16]) he applied Hansen's work to ruled surfaces and he explicitly calculated parameters for certain codes on ruled surfaces over curves of genus 0 and 1. Before studying the ruled surface we introduce here the projective space bundle. We will see that space bundles associated to ruled surfaces give an important invariant for the surfaces.

Definition 6.1 *Let $(X, \mathcal{O}_X)$ be a ringed space, $\mathcal{F}$ a sheaf of $\mathcal{O}_X$-modules. The **symmetric algebra** $\mathcal{S}(\mathcal{F})$ of $\mathcal{F}$ is the sheaf associated to the preasheaf which assigns to every open set U the symmetric algebra of $\mathcal{F}(U)$ over $\mathcal{O}_X(U)$.*

Suppose X is a noetherian scheme and $\mathcal{S}$ is a sheaf of graded $\mathcal{O}_X$-algebras satisfying the following condition:

(✠) $\mathcal{S} \cong \bigoplus_{d\geq 0} \mathcal{S}_d$ where $\mathcal{S}_d$ is the homogeneous part of degree d. Suppose also $\mathcal{S}_0 = \mathcal{O}_X$, $\mathcal{S}_1$ is a coherent $\mathcal{O}_X$-module and $\mathcal{S}$ is locally generated by $\mathcal{S}_1$ as $\mathcal{O}_X$-algebra.

For every open affine subset $U = \operatorname{Spec} A \subset X$, put $\mathcal{S}(U) = \Gamma(U, \mathcal{S}_{|U})$. $\mathcal{S}(U)$ is a graded A-algebra generated by $\mathcal{S}_1(U)$. We can consider $\operatorname{Proj} \mathcal{S}(U)$ and the natural morphism $\pi_U : \operatorname{Proj} \mathcal{S}(U) \to U$. If $f \in A$ and U_f is the principal affine open subset $\operatorname{Spec} A_f$, then, since $\mathcal{S}$ is coherent, we have $\pi^{-1}(\operatorname{Spec} U_f) \cong \operatorname{Proj} S(U_f)$. Then, for two open affine subsets U and V, we have $\pi_U^{-1}(U \cap V) \cong \pi_V^{-1}(U \cap V)$. So the maps $\pi_U : \operatorname{Proj} \mathcal{S}(U) \to U$ can be glued to obtain a scheme $\operatorname{Proj} \mathcal{S} \to X$ such that $\pi^{-1}(U) \cong \operatorname{Proj} \mathcal{S}(U)$ for every open affine subset U. Also the invertible sheaves $\mathcal{O}(1)$ on each $\operatorname{Proj} \mathcal{S}(U)$ can be glued together to obtain an invertible sheaf $\mathcal{O}(1)$ on $\operatorname{Proj} \mathcal{S}$.

EXAMPLE: If S is the $\mathcal{O}_X$-algebra $\mathcal{S} = \mathcal{O}_X[T_0, \cdots, T_n]$, then $\operatorname{Proj} \mathcal{S}$ is $\mathbb{P}^n_X$ with the twisting sheaf $\mathcal{O}(1)$ defined in definition 4.6.

Definition 6.2 *Let X be a noetherian scheme, and $\mathcal{E}$ be a locally free coherent sheaf on X. The **projective space bundle** $\mathbf{P}(\mathcal{E})$ is defined as $\mathbf{P}(\mathcal{E}) = \operatorname{Proj} \mathcal{S}(\mathcal{E})$.*

REMARK: $\mathcal{S}(\mathcal{E})$ satisfies the condition ✠. Indeed, take U such that E is free over U. Then $\mathcal{S}(\mathcal{E})_{|U} \cong S(\mathcal{O}_U^n) \cong \mathcal{O}_U[T_1, \cdots, T_n]$. Thus $\pi_U^{-1} \cong \operatorname{Proj} \mathcal{O}_U[T_1, \cdots, T_n] = \mathbb{P}^{n-1}$.

Proposition 6.1 *Let X, $\mathcal{E}$, $\mathbf{P}(\mathcal{E})$ be as in the definition. If $\operatorname{rank} \mathcal{E} \geq 2$ there is a canonical isomorphism of graded O_X-algebras $\mathcal{S}(\mathcal{E}) \cong \bigoplus_{l\in\mathbb{Z}} \pi_*(\mathcal{O}(l))$.*

Proposition 6.2 *Let X, $\mathcal{E}$, $\mathbb{P}(\mathcal{E})$ be as before. Let $g : Y \to X$ be any morphism. Then there is a one-to-one correspondence between X-morphisms from Y to $\mathbf{P}(\mathcal{E})$ and invertible sheaves $\mathcal{L}$ on Y together with a surjective map of sheaves $g^*\mathcal{E} \to \mathcal{L}$. The invertible sheaf corresponding to a morphism f is $\mathcal{L} = f^*(\mathcal{O}(1))$.*

6.2 Ruled surfaces

In this paragraph ruled surfaces are defined and their fundamental properties are presented. In particular we investigate the relations between objects concerned a ruled surface and objects defined over the underlying projective curve.

NOTE: In the following we will use the word "vector bundle" as synonym of "locally free sheaf" and "line bundle" for "invertible sheaf". See also the note at page 49.

Definition 6.3 *A **ruled surface** over a nonsingular curve C is a surface X with a morphism $\pi : X \to C$, such that for every $y \in C$ the fiber $X_y = X \times_C K(y)$ is isomorphic to $\mathbb{P}^1$ and such that π admits a section, i.e. a morphism $\sigma : C \to X$ with $\pi\sigma = id_C$.*

FACT: The fibers are numerically equivalent. We did not define here the Neron-Severi group, but this fact comes easily by observing that the fibers are parametrized by a curve, and algebraically equivalent divisors are numerically equivalent.

EXAMPLE: The easiest example of ruled surface over a curve C is given by $\mathbb{P}^1 \times C$ with the second projection.

The next results show that many properties of the ruled surfaces can be deduced from the properties of the underlying curve. This is one of the reasons why, studying codes on surfaces, we chose to start from codes on ruled surfaces. In fact, many problems can be reduced to problems about curves, and the geometry of curves is easier than the geometry of higher dimensional varieties.

Lemma 6.1 *Let $\pi : X \to C$ be a ruled surface, let D be a divisor on X with $D.f = n \geq 0$ for a fiber f of π. Then $\pi_*\mathcal{L}(D)$ is a vector bundle of rank $n+1$ on C. In particular $\pi_*\mathcal{O}_X = \mathcal{O}_C$.*

The next proposition is the fundamental link between the theory of ruled surfaces and the study of rank 2 vector bundles over curves.

Proposition 6.3 *If $\pi : X \to C$ is a ruled surface, then there exists a vector bundle $\mathcal{E}$ of rank 2 over C, such that $X \cong \mathbf{P}(\mathcal{E})$. Conversely, for every vector bundle $\mathcal{E}$ of rank 2 over C, $\mathbf{P}(\mathcal{E})$ is a ruled surface over X. $\mathbf{P}(\mathcal{E}) \cong \mathbf{P}(\mathcal{E}')$ if and only if $\mathcal{E}' \cong \mathcal{E} \otimes \mathcal{L}$ for a line bundle $\mathcal{L}$ over C.*

Proposition 6.4 *Let $\pi : X \to C$ be a ruled surface, f a fiber, $C_0 = \sigma(C) \subset X$ for a section σ. Then*

$$Pic(X) \cong \mathbb{Z} \oplus \pi^* Pic(C),$$

where $\mathbb{Z}$ is generated by C_0.

$$Num(X) \cong \mathbb{Z} \oplus \mathbb{Z},$$

generated by C_0, f and with $C_0.f = 1$, $f.f = 0$.

In the following we will use the next lemma to compute the dimension of the codes on ruled surfaces.

Lemma 6.2 *Let D be a divisor on X, with $D.f \geq 0$ for a fiber f. Then $H^i(X, \mathcal{L}(D)) \cong H^i(C, \pi_* \mathcal{L}(D))$.*

Corollary 6.1 *If the genus of C is g, then $p_a(X) = -g$, $p_g(X) = 0$, $h^1(X, \mathcal{O}_X) = g$.*

Proof: By Lemmas 6.1 and 6.2, $h^1(X, \mathcal{O}_X) = h^1(C, \pi_* \mathcal{O}_X) = h^1(C, \mathcal{O}_C) = g$, $p_g = h^2(X, \mathcal{O}_X) = h^2(C, \pi_* \mathcal{O}_X) = h^2(C, \mathcal{O}_C) = 0$, $p_a = p_g - h^1(X, \mathcal{O}_X) = -g$. □

Let us go back to study rank 2 vector bundles on curves.

Definition 6.4 *A vector bundle $\mathcal{E}$ of rank 2 over a curve C is said to be **normalized** if $H^0(C, \mathcal{E}) \neq 0$ and $H^0(C, \mathcal{E} \otimes \mathcal{L}) = 0$ for every line bundle $\mathcal{L}$ with $\deg \mathcal{L} < 0$.*

Definition 6.5 *The degree of a vector bundle $\mathcal{E}$ of rank n over C is the degree of the line bundle $\Lambda^n \mathcal{E}$ over C.*

More generally we could define the degree of a coherent sheaf over a non-singular projective curve, as in [7, II ex 2.16]. In the case of vector bundles the two definitions would be compatible.

Proposition 6.5 *Let $\pi : X \to C$ be a ruled surface. It is possible to write $X \cong \mathbb{P}(\mathcal{E})$ with $\mathcal{E}$ normalized. For such $\mathcal{E}$, the integer $e = -\deg \mathcal{E}$ is an invariant of X and there exists a section $\sigma_0 : C \to X$ with image C such that $\mathcal{L}(C_0) \cong O_X(1)$.*

In the following, $\pi : X \to C$ is a ruled surface, $X = \mathbb{P}(\mathcal{E})$ with $\mathcal{E}$ normalized, $\mathbf{e} = \Lambda^2\mathcal{E}$, $e = -\deg \mathbf{e}$. We fix a section C_0 such that $\mathcal{L}(C_0) \cong \mathcal{O}_X(1)$. We remind that, by Proposition 6.2, every section of X corresponds to a surjection from $\mathcal{E}$ to an line bundle $\mathcal{L}$ on C, given by $\mathcal{L} = \sigma^*\mathcal{O}_X(1)$. Indeed a section can be considered as a morphism of C-schemes from C to $\mathbb{P}(\mathcal{E}) = X$.

Proposition 6.6 *If D is a section of X, corresponding to a surjection $\mathcal{E} \to \mathcal{L}(\mathbf{d})$ for some $\mathbf{d} \in Div(C)$, then $\deg \mathbf{d} = C_0.D$ and $D \approx C_0 + \pi_*(\mathbf{d} - \mathbf{e})$. In particular $C_0.C_0 = \deg \mathbf{e} = -e$.*

Lemma 6.3 *Let W be the canonical divisor on X, $\mathbf{w}$ the canonical divisor on C. Then $W \approx -2C_0 + \pi_*(\mathbf{w} + \mathbf{e})$, $W \equiv -2C_0 + (2g - 2 - e)f$.*

Proof: We know that $W \equiv aC_0 + bf$ for some $a, b \in \mathbb{Z}$. Using adjunction formula for a the fiber f we get $-2 = f.f(f+W) = f.(f+aC_0+bf) = af C_0$ as f is isomorphic to $\mathbb{P}^1$. Now write $W \approx -2C_0+\pi^*(\mathbf{b})$ for some $\mathbf{b} \in Div(C)$. By Proposition 5.2, $\omega_{C_0} \cong \omega_X \otimes \mathcal{L}(C_0) \otimes \mathcal{O}_{C_0} \cong \mathcal{L}(W + C_0) \otimes \mathcal{O}_{C_0} \cong \mathcal{L}(-C_0 + \pi^*\mathbf{b}) \otimes \mathcal{O}_{C_0}$. Identifying C_0 with C via π, we have $\mathbf{w} = -\mathbf{e} + \mathbf{b}$, so $+\mathbf{b} = \mathbf{w} + \mathbf{e}$. To conclude, $\deg(\mathbf{w} + \mathbf{e}) = 2g - 2 - e$. □

Definition 6.6 *A vector bundle is called **decomposable** if it can be written as direct sum of vector bundles of smaller rank.*

Theorem 6.1 *Let X, C, $\mathcal{E}$, e be as before. Then*

1. *If $\mathcal{E}$ is decomposable then $\mathcal{E} \cong \mathcal{O}_C \oplus \mathcal{L}$ for some $\mathcal{L}$ with $\deg \mathcal{L} \leq 0$. Therefore $e \geq 0$. All the values of $e \geq 0$ are possible.*
2. *If $\mathcal{E}$ is indecomposable then $-g \leq e \leq 2g - 2$.*

Since our purpose is to apply Hansen's results (Proposition 5.6 and Lemma 5.4) to ruled surfaces, we need a criterion for ample and nef divisors on ruled surfaces. The following theorem comes from [7], except part (1), that can be found in [9].

Theorem 6.2 *Suppose now that X and C are defined over a field of characteristic p. Using the usual notation, define*

$$k = \begin{cases} e & \text{if } e \geq 0 \\ \frac{1}{2}e & \text{if } e < 0 \text{ and } g \geq 1 \\ \frac{1}{2}e + \frac{g-1}{p} & \text{if } e < 0 \text{ and } g > 1. \end{cases}$$

If $D \equiv aC_0 + bf$ then

1. *If $\mathcal{E}$ is the direct sum of two ample line bundles on C, then C_0 is ample.*
2. *If $e \geq 0$ and $Y \not\equiv C_0$ is an irreducible curves on C with $Y \equiv D$, then $a > 0$ and $b \geq ak$.*

3. *(**Case 1**: $e \geq o$ or $g \leq 1$)*
   D is ample (resp. nef) if and only if $a > 0$ and $b > ak$ (resp. $a \geq 0$ and $b \geq ak$).

4. *(**Case 2**: $e < o$ and $g > 1$)*
   If D is ample (resp. nef) then $a > 0$ and $b > \frac{1}{2}ae$ (resp. $a \geq 0$ and $b \geq \frac{1}{2}ae$). If $a > 0$ and $b > ak$ then D is ample.

6.3 Parameters of codes on ruled surfaces

We have now the tools needed to prove the fundamental result about codes on ruled surfaces. The following theorem is mainly due to Hansen [6, Prop. 4.1], but Lomont corrected some mistakes [16, Remark 5.1.5]. In particular, [6] does not assume $\mathcal{E}$ to be normalized .

Theorem 6.3 (Hansen-Lomont) *Let C be a nonsingular curve of genus g, $\mathcal{E}$ a normalized vector bundle of rank 2 over C, $X = \mathbf{P}(\mathcal{E})$ the associated ruled surface $\pi : \mathbf{P}(\mathcal{E}) \to C$ with invariant e, f is a fiber over a point $P_0 \in C$ and $\gamma = \#C(\mathbb{F}_q)$. Fix integers $a \geq 0$ and $b \geq 0$. If $\mathcal{E}$ is not ample put $m = a(\lceil k \rceil - e) + b$, otherwise $m = b - ae$. If $m < \gamma$ and $\gamma(q+1) \geq (\gamma - m)a + (q+1)m$ then there are codes with parameters*

$$n = (q+1)\gamma$$

$$\mathrm{k} = h^0(C, S^a(\mathcal{E}) \otimes \mathcal{L}_C(bP_0))$$

$$d \geq n - (\gamma - m)a - (q+1)m \ .$$

Proof: We apply Proposition 5.6 to the fibers $f_1, \cdots, f_\gamma$ over the γ rational points of C. We get $n = (q+1)\gamma$, as $f_i \cong \mathbb{P}^1$. Let $D \equiv aC_0 + bf$ and $\mathcal{L} = \mathcal{L}(D)$. By Propositions 6.2 and 6.1

$$\Gamma(X, \mathcal{L}) \cong \Gamma(C, \pi_*\mathcal{L}) \cong \Gamma(S^a(\mathcal{E}) \otimes \mathcal{L}_C(bC_0)) \ .$$

Now we apply Corollary 5.4 to $H = C_0 + \lceil k \rceil f$ and so we get that H is nef, $H.f_i = 1$, $D.f_i = a$ and $H.D = a(\lceil k \rceil - e) + b$. So

$$l \leq \frac{D.H}{\min\{f_i.H\}} = a(\lceil k \rceil - e) + b \ .$$

If $\mathcal{E}$ is ample then C_0 is nef so, applying the corollary with $H = C_o$, we have $l = H.D = b - ae$. Remark that $n \geq (\gamma - m)a + (q+1)m$ ensures the injectivity of the germ map α. Moreover, $m < \gamma$ implies that $a < q + 1 = \gamma$, so we conclude that $d \geq n - (\gamma - m)a - (q+1)m$. □

6.4 Codes on rational ruled surfaces

In this subsection we follow [16] and we apply Theorem 6.3 to codes over rational ruled surfaces, i.e. ruled surfaces over $\mathbb{P}^1$. As we already saw, this means to study the vector bundles of rank 2 over $\mathbb{P}^1$. We first observe that a vector bundle $\mathcal{E}$ of rank 2 over $\mathbb{P}^1$ cannot be indecomposable, otherwise the invariant e is between 0 and -2, by Theorem 6.1. So $\mathcal{E} \cong \mathcal{O}_C \oplus \mathcal{L}$ for any line bundle $\mathcal{L}$ with $\deg \mathcal{L} \leq 0$. But $\operatorname{Pic} \mathbb{P}^1 \cong \mathbb{Z}$, generated by a hyperplane, so $\mathcal{L} \cong \mathcal{O}_C(-e)$ for any $e \geq 0$. $\mathbb{P}^1$ has $q+1$ points, hence, applying Theorem 6.3, $n = (q+1)^2$. Since $\mathcal{O}_C \oplus \mathcal{O}_C(-e)$ is not ample, we get $m = a(\lceil k \rceil - e) + b = e$. We require $b = m < \gamma = q+1$ and $n > (\gamma - m)a + (q+1)m$. This is equivalent to ask for $a < q+1$ and $b < q+1$. This way we get $d \geq (q+1)^2 - (q+1-b)a - (q+1)b = (q+1-a)(q+1-b)$.

We have now to estimate the dimension $\mathrm{k} = h^0(C, S^a(\mathcal{E}) \otimes \mathcal{L}_C(bP_0))$.
We know, for two sheaves $\mathcal{F}$ and $\mathcal{F}'$, that

$$S^a(\mathcal{F} \oplus \mathcal{F}') = \bigoplus_{n+m=a} (S^n(\mathcal{F}) \otimes S^m(\mathcal{F}')).$$

Therefore

$$S^a(\mathcal{O}_C \oplus \mathcal{O}_C(-e)) = \bigoplus_{j=0}^{a} (S^{a-j}\mathcal{O}_C \otimes S^j(\mathcal{O}_C(-e))) = \bigoplus_{j=0}^{a} \mathcal{O}_C(-ej).$$

Since cohomology commutes with direct sums, we get

$$\mathrm{k} = \sum_{j=0}^{a} h^0(C, \mathcal{L}_C((b-ej)P_0)).$$

If $b - ej < 0$ then $H^0(C, \mathcal{L}_C((b-ej)P_0)) = \{0\}$, otherwise, by the Riemann-Roch theorem, $h^0(C, \mathcal{L}_C((b-ej)P_0)) = b - ej + 1$. We finally obtain that $\mathrm{k} = \sum b - ej + 1$, where the sum is over j such that $j \leq a$, $ej \leq b$. Fixing e, by increasing a and b, we increase k, but, as often happens in coding theory, we decrease the distance. Conversely, fixing a and b, we get the biggest dimension for $e = 0$, while d does not depend on e.

We summarize these results in the following theorem:

Theorem 6.4 (Lomont) *Let $C = \mathbb{P}^1$, $\mathcal{E}$ the normalized vector bundle $\mathcal{O}_C \oplus \mathcal{O}_C(-e)$, where $e \geq 0$, X the associated ruled surface $\mathbf{P}(\mathcal{E})$. Then, for any integers $0 \leq a, b \leq q+1$, there exist AG codes over X with parameters*

$$n = (q+1)^2$$

$$d \geq (q+1-a)(q+1-b)$$

$\bar{\mathbf{R}}$	$\mathbf{k_1}$	$\mathbf{k_2}$	**rate**	δ	**a**	**b**	**rate**	δ
0.1	81	81	0.1009	0.470973	81	81	0.100562	0.47165
0.2	115	114	0.201615	0.307912	114	114	0.20023	0.309603
0.3	140	140	0.301423	0.206936	140	140	0.301004	0.207255
0.4	162	161	0.401107	0.137332	162	161	0.402262	0.136641
0.5	181	180	0.501038	0.0876586	181	180	0.501506	0.0874502
0.6	198	198	0.602907	0.0517339	199	198	0.602583	0.05181
0.7	214	213	0.700992	0.0277739	215	213	0.703114	0.0273433
0.8	229	228	0.802953	0.0116263	229	228	0.800921	0.01187
0.9	242	242	0.900638	0.00301423	243	242	0.901391	0.00296749

Table 1: Comparison between product of two Reed-Solomon codes and the code produced by Theorem 6.4.

$$\mathrm{k} = \sum (b - ej)$$

where the sum is over j such that $j \leq a$, $ej \leq b$. The highest rate is for $e = 0$. In that case we have

$$n = (q+1)^2$$

$$d \geq (q+1-a)(q+1-b)$$

$$\mathrm{k} = (a+1)(b+1)$$

$$X \cong \mathbb{P}^1 \times \mathbb{P}^1.$$

We check now the efficiency of the codes. As the code with the best rate is constructed on the surface $\mathbb{P}^1 \times \mathbb{P}^1$, it is natural to compare the parameters of the new code with those of a well-known code, namely the product codes of two Reed-Solomon codes (see [25]). Indeed it can be proved that a Reed-Solomon is an algebraic geometric code over $\mathbb{P}^1$. The product code of two Reed-Solomon codes over $\mathbb{F}_q$ is a $[n, \mathrm{k}, d]$-code, with $n = (q-1)^2$, $\mathrm{k} = k_1 k_2$, $d \geq (q-k_1)(q-k_2)$ for $0 \leq k_1, k_2 \leq q-1$. We fix a rate $\bar{R} = \mathrm{k}/n$ and let k_1, k_2 run to get the code with highest relative distance $\delta = d/n$ and rate at least $\bar{R}$. Then we do the same for the codes of Theorem 6.4. In the following table we show the rates and the relative distances and the corresponding k_1, k_2 and a, b for every $\bar{R}$. We set $q = 256$.
We can observe that in 6 cases, the codes produced by Theorem 6.4 are more efficient than the product codes. Moreover, since they are longer, they can better correct burst error.

6.5 Computing the dimension in the decomposable case

For a positive genus curve we cannot say that all the vector bundles of rank 2 over it are decomposable and all the decomposable ones are isomorphic

to $\mathcal{O}_C \oplus \mathcal{O}_C(-e)$, but we can extend the reasoning done for rational ruled surfaces to study the codes produced by decomposable vector bundles of the form $\mathcal{O}_C \oplus \mathcal{O}_C(-e)$. The only difference is that, evaluating the dimension of the code, we have to consider also the spaces $H^0(C, W - \mathcal{O}_C(b - je))$ in the Riemann-Roch theorem, where W is the canonical divisor on C. We obtain the following theorem:

Theorem 6.5 (Lomont) *Let C be a smooth curve of positive genus g, $\mathcal{E} = \mathcal{O}_C \oplus \mathcal{O}_C(-e)$ for an integer $e \geq 0$, X the corresponding ruled surface. Indicate with γ the number of $\mathbb{F}_q$-rational points of C. For every integers $0 \leq a < q+1$ and $0 \leq b < \gamma$, the codes produced by Theorem 6.3 have parameters*

$$n = (q+1)\gamma$$

$$d \geq (q+1-a)(\gamma - b)$$

$$\mathrm{k} = \sum (b - je - g + 1 + h^0(C, W - \mathcal{O}_C(b - je)))$$

where the sum is over j such that $j \leq a$, $ej \leq b$ and W is the canonical divisor on C. The highest rate is for $e = 0$. In that case we have

$$n = (q+1)\gamma$$

$$d \geq (q+1-a)(\gamma - b)$$

$$\mathrm{k} = (a+1)(b+1-g+h^0(C, W - \mathcal{O}_C(b)))$$

$$X \cong \mathbb{P}^1 \times C.$$

REMARK: Clearly, if we take $b > 2g-2$, the dimension is simply $(a+1)(b+1-g)$.

For example, take the Klein quartic C at page 36 and compute the parameters of the codes over $\mathbb{P}^1 \times C$, i.e. over the ruled surface associated to the normalized decomposable bundle $\mathcal{O}_C \oplus \mathcal{O}_C$. C has genus 3 and 17 rational points over $\mathbb{F}_{16}$, therefore $n = 289$. Fixed a minimum rate $\bar{R}$, we can let a and b run and find the code with the highest relative dimension k/n and rate $\delta = d/n$ greater or equal $\bar{R}$. The results are shown in table 2.

6.6 Computing the dimension in the general case

We saw that our main problem is to compute the dimension of the codes on ruled surfaces i.e. to compute $h^0(S^a(\mathcal{E}) \otimes \mathcal{O}_C(bP_o))$. Lomont does not say anything about h^0 in the general case. He treats just the decomposable case for curves of any genus and the only theorem for curves of genus greater

$\bar{\mathbf{R}}$	**a**	**b**	**rate**	δ
0.1	5	7	0.103806	0.415225
0.2	9	8	0.207612	0.249135
0.3	10	10	0.304498	0.16955
0.4	12	11	0.404844	0.103806
0.5	13	13	0.532872	0.0553633
0.6	14	14	0.622837	0.0311419
0.7	15	15	0.719723	0.0138408
0.8	16	16	0.823529	0.00346021

Table 2: Efficiency of a code produced by Theorem 6.5 for a ruled surface over the Klein quartic.

than 1 is Theorem 6.3. In this subsection we investigate the general case and we prove a theorem about the parameters of codes on ruled surfaces associated to suitable rank 2 vector bundles. .

For decomposable vector bundles we reduced to an easy problem, namely the calculation of the h^0 of a line bundle. When we deal with indecomposable vector bundle we cannot use this approach anymore, and we need more information about the global sections of vector bundles. The fundamental result is again a Riemann-Roch theorem, generalized to vector bundles over curves and often called Weil-Riemann-Roch theorem.

Theorem 6.6 (Weil-Riemann-Roch) *Let $\mathcal{F}$ be a vector bundle of rank r and degree d over a smooth projective curve of genus g. Then*

$$h^0(C,\mathcal{F}) - h^1(C,\mathcal{F}) = d + r(1-g).$$

Using Serre's duality theorem, we can write $h^1(C,\mathcal{F})$ as $\dim Hom(\mathcal{F},\Omega_C)$, where Ω_C is the sheaf of differentials. See [13, th. 8.5.4 p. 108].

It is clear that we have to know degree and rank of the vector bundle $S^a(\mathcal{E}) \otimes \mathcal{O}_C(bP_0)$. This can be done by using the following well-known theorems, whereby proofs can be found for instance in the appendix of [16].

Theorem 6.7 *For vector bundles $\mathcal{E}$ and $\mathcal{F}$ over a curve C*

$$\deg(\mathcal{E}\otimes\mathcal{F}) = \operatorname{rank}\mathcal{F}\deg\mathcal{E} + \operatorname{rank}\mathcal{E}\deg\mathcal{F}.$$

Theorem 6.8 *If $\mathcal{E}$ is a rank r degree d vector bundle over a curve C, then*

$$\operatorname{rank} S^n(\mathcal{E}) = \binom{n+r-1}{r-1}.$$

Theorem 6.9 *If $\mathcal{E}$ is a rank r degree d vector bundle over a curve C, then*

$$\deg S^n(\mathcal{E}) = \frac{dn}{r}\binom{n+r-1}{r-1}.$$

The theorems above lead immediately to the following proposition:

Proposition 6.7 *Let $\mathcal{E}$ be a rank 2 degree d vector bundle over a smooth projective curve of genus g. Then*

$$h^0(C, S^a(\mathcal{E}) \otimes \mathcal{O}_C(bP_0)) = h^1(C, S^a(\mathcal{E}) \otimes \mathcal{O}_C(bP_0)) + (a+1)(b + \frac{da}{2} + 1 - g).$$

REMARK: Proposition 6.7 is compatible with the previous calculation of $h^0(\mathbb{P}^1, S^a(\mathcal{O}_C \oplus \mathcal{O}_C) \otimes \mathcal{O}_C(bP_0))$, since the first cohomology group is 0.

We can observe that, even if we cannot compute the dimension of codes on a ruled surface, we already have a lower bound for it. The last missing step in order to compute its exact value is the knowledge of $h^1((S^n(\mathcal{F}_r) \otimes \mathcal{O}_C(bP_0))$. In the following we give some further conditions to calculate exactly $h^0((S^n(\mathcal{F}_r) \otimes \mathcal{O}_C(bP_0))$. In particular, we study some sufficient conditions to make $h^1((S^n(\mathcal{F}_r) \otimes \mathcal{O}_C(bP_0))$ vanish.

At page 45 we said that every coherent sheaf can be written as a quotient of a direct sum of twisted sheaves. Looking at the proof we can state this result more precisely.

Proposition 6.8 *Let $\mathcal{F}$ be a coherent sheaf over a projective scheme X and let n be such that $\mathcal{F}(n)$ is generated by global sections. Then $\mathcal{F}$ is isomorphic to the quotient of a direct sum of copies of $\mathcal{O}_X(-n)$.*

Proof: If $\mathcal{F}(n)$ is generated by global sections, it means there exists a surjection $\bigoplus \mathcal{O}_X \to \mathcal{F}(n)$. Tensoring with $\mathcal{O}_X(-n)$ we get a surjection from $\bigoplus \mathcal{O}_X(-n) \to \mathcal{F}$. □

Corollary 6.2 *Let $\mathcal{F}$ be a vector bundle over a smooth projective curve C of genus g and let n be such that $\mathcal{F}(n)$ is generated by global sections. Then $h^1(C, \mathcal{F} \otimes \mathcal{L}) = 0$ for every line bundle with $\deg \mathcal{L} > 2g - 2 + n$.*

Proof: We know that $h^1(C, \mathcal{O}_X(-n) \otimes \mathcal{L}) = 0$ if $\deg \mathcal{L} - n > 2g - 2$. Since the cohomology commutes with the direct sums, if $\deg \mathcal{L} > n + 2g - 2$ then $h^1(C, \bigoplus \mathcal{O}_X(-n) \otimes \mathcal{L}) = \sum h^1(C, \mathcal{O}_X(-n) \otimes \mathcal{L}) = 0$. If we write the exact sequence

$$0 \longrightarrow \mathcal{I} \otimes \mathcal{L} \longrightarrow \bigoplus \mathcal{O}_X(-n) \otimes \mathcal{L} \longrightarrow \mathcal{F} \otimes \mathcal{L} \longrightarrow 0$$

we get the exact cohomology sequence

$$\cdots \longrightarrow H^1(C, \bigoplus \mathcal{O}_X(-n) \otimes \mathcal{L}) \longrightarrow H^1(C, \mathcal{F} \otimes \mathcal{L}) \longrightarrow 0$$

as higher degree terms vanish by the Grothendieck vanishing theorem, so we can conclude. □

Corollary 6.3 *Let $\mathcal{E}$ be a rank 2 vector bundle over a smooth projective curve C of genus g and let n be such that $\mathcal{E}(n)$ is generated by global sections. Then $h^1(C, S^a(\mathcal{E}) \otimes \mathcal{O}_C(bP_0)) = 0$ for $b > 2g - 2 + na$.*

Proof: $\mathcal{E}^{\otimes a}(na)$ is generated by global sections, so also $S^a(\mathcal{E})(na)$. □

Corollary 6.4 *Let $\mathcal{E}$ be a vector bundle over a smooth projective curve C of genus g, $\mathcal{E}$ generated by global sections. Then $h^1(C, S^a(\mathcal{E}) \otimes \mathcal{O}_C(bP_0)) = 0$ for $b > 2g - 2$.*

Another sufficient condition is related to the concepts of stability and semistability, introduced by Mumford.

Definition 6.7 *A vector bundle $\mathcal{E}$ is called **stable** if, for every proper subbundle $\mathcal{F}$ of $\mathcal{E}$,*

$$\frac{\deg \mathcal{F}}{\operatorname{rank} \mathcal{F}} < \frac{\deg \mathcal{E}}{\operatorname{rank} \mathcal{E}}.$$

*It is called **semistable** if*

$$\frac{\deg \mathcal{F}}{\operatorname{rank} \mathcal{F}} \leq \frac{\deg \mathcal{E}}{\operatorname{rank} \mathcal{E}}.$$

Lemma 6.4 *We have the following:*

1. *Every line bundle $\mathcal{L}$ is stable*
2. *If $\mathcal{E}$ is stable (resp. semistable) then $\mathcal{E} \otimes \mathcal{L}$ is stable (resp. semistable).*

Proposition 6.9 *Let $\mathcal{E}$ be a vector bundle of rank r and degree d over a smooth projective curve C of genus g.*

1. *If $\mathcal{E}$ is stable and $d \geq r(2g-1)$ then $\mathcal{E}$ is generated by global sections.*
2. *If $\mathcal{E}$ is stable and $d \geq r(2g-2)$ then $h^1(C, \mathcal{E}) = 0$.*
3. *If $\mathcal{E}$ is semistable and $d > r(2g-1)$ then $\mathcal{E}$ is generated by global sections.*
4. *If $\mathcal{E}$ is semistable and $d > r(2g-2)$ then $h^1(C, \mathcal{E}) = 0$.*

Proof: Good and clear references are the notes by Montserrat Teixidor I Bigas on Vector bundles on curves, used for the Boston and Tufts Universities seminar on vector bundles on curves. They can be found at the web address http://www.tufts.edu/~mteixido/files/vectbund.pdf

We can summarize these results in the following theorem:

Theorem 6.10 (Zampolini) *Let C be a nonsingular curve of genus g, $\mathcal{E}$ a normalized vector bundle of rank 2 over C, $X = \mathbf{P}(\mathcal{E})$ the associated ruled surface $\pi : \mathbf{P}(\mathcal{E}) \to C$ with invariant e. f is a fiber over a point $P_0 \in C$ and $\gamma = \#C(\mathbb{F}_q)$. Fix integers $a \geq 0$ and $b \geq 0$. If $\mathcal{E}$ is not ample put $m = a(\lceil k \rceil - e) + b$, otherwise $m = b - ae$. If $m < \gamma$ and $\gamma(q+1) \geq (\gamma - m)a + (q+1)m$ then there are codes with parameters*

$$n = (q+1)\gamma$$

$$\mathrm{k} \geq (a+1)(b - \frac{ea}{2} + 1 - g)$$

$$d \geq n - (\gamma - m)a - (q+1)m \ .$$

Moreover if at least one of the following conditions

1. *$\mathcal{E}$ is generated by global sections and $b > 2g - 2$,*
2. *$\mathcal{E}(n)$ is generated by global sections and $b > 2g - 2 + na$,*
3. *$\mathcal{E}$ is semistable and $-e > 4g - 1$,*
4. *$\mathcal{E}$ is stable and $-e \geq 4g - 1$,*

holds then $\mathrm{k} = (a+1)(b - \frac{ea}{2} + 1 - g)$.

6.7 Ruled surfaces over elliptic curves

We saw that for rational ruled surfaces the only possible codes are those generated by decomposable vector bundles of rank 2. Next step is to study rank 2 vector bundles over elliptic curves. The decomposable case has been treated in Theorem 6.5, so we can focus on rank 2 normalized indecomposable vector bundles $\mathcal{E}$ over elliptic curves. By Theorem 6.1, if $\mathcal{E}$ is normalized, then either $\deg \mathcal{E} = 0$ or $\deg \mathcal{E} = 1$. Viceversa, Hartshorne in [7, V 2.15] proves that if X is a ruled surface over an elliptic curve C, corresponding to an indecomposable $\mathcal{E}$, then $e = 0$ or -1, and there is exactly one such ruled surface over C for each of these two values of e. The computation of $h^0(C, S^a(\mathcal{E}) \otimes \mathcal{O}_C(bP_0))$ in the degree 0 case is solved in Lomont's PhD thesis, while Lomont leaves the degree 1 case as an open problem. We were able to partially solve this case for some a and b, while the general case, for arbitrary a and b, is still open.

The solution of degree zero case uses deep results about vector bundles over elliptic curves. The classification of vector bundles over elliptic curves defined over an algebraically closed field of zero characteristic is due to Atiyah ([1]). Arason, Elman and Jacob extended in [11] such results to elliptic curves over perfect fields, hence to finite fields. We refer to these references for a proof of the following theorem.

Theorem 6.11 (Atiyah-Arason-Elman-Jacob) *Let C be an elliptic curve over a perfect field K. Denote by $E(r,d)$ the set of indecomposable vector bundles of rank r and degree d over C. We have that:*

1. *It is possible to associate to each K-rational point $P \in C$ a vector bundle $\mathcal{E}_{r,d,P} \in E(r,d)$;*
2. *$\mathcal{E}_{r,d,P} \cong \mathcal{E}_{r,d,P}$ if and only if $P = Q$;*
3. *Every $\mathcal{M} \in E(r,d)$ is of the form $\mathcal{E}_{r,d,P}$ for some $P \in C$;*
4. *For every r there exists a vector bundle $\mathcal{F}_r \in E(r,0)$, unique up to isomorphism, with $\Gamma(X,\mathcal{F}_r) \neq 0$. Moreover we have an exact sequence*

$$0 \to \mathcal{O}_C \to \mathcal{F}_r \to \mathcal{F}_{r-1} \to 0$$

   and $\Gamma(X,\mathcal{F}_r) = K$;

5. *Let $\mathcal{E} \in E(r,0)$. Then $\mathcal{E} \cong \mathcal{L} \otimes \mathcal{F}_r$, where $\mathcal{L}$ is a line bundle of degree 0;*
6. *$\dim \Gamma(\mathcal{F}_r \otimes \mathcal{F}_s) = \min\{r,s\}$. If $\mathcal{L}$ is a line bundle then $\dim \Gamma(\mathcal{L} \otimes \mathcal{F}_r \otimes \mathcal{F}_s) = 0$ unless $\deg L > 0$;*
7. *If $2 \leq s \leq r$ then $\mathcal{F}_r \otimes \mathcal{F}_s = \bigoplus_{i=1}^{s} \mathcal{F}_{r-s+2i-1}$.*

We have now the tools needed to prove the following proposition about the structure of $S^n(\mathcal{F}_r)$.

Proposition 6.10 (Lomont) *Let $\mathcal{F}_r$ be as in Theorem 6.11. Then $S^n(\mathcal{F}_r) = \mathcal{F}_{r_i} \oplus \cdots \oplus \mathcal{F}_{r_j}$ for some $\mathcal{F}_{r_i}$, with $r_1 + \cdots + r_j = \binom{n+r-1}{r-1}$.*

Proof: Write $S^n(\mathcal{F}_r) = \bigoplus \mathcal{E}_i$, where $\mathcal{E}_i$ are the indecomposable components. Take a line bundle $\mathcal{L}$ of degree zero over C with $H^0(C,\mathcal{L}) = 0$ and consider the exact sequence

$$0 \longrightarrow \mathcal{I} \longrightarrow \mathcal{F}_r^{\otimes n} \longrightarrow S^n(\mathcal{F}_r) \longrightarrow 0.$$

Since $\deg \mathcal{F}_r = 0$, we deduce from Theorems 6.7 and 6.9 that $\deg \mathcal{F}_r^{\otimes n} = 0$ and $\deg S^n(\mathcal{F}_r) = 0$, so $\deg \mathcal{I} = 0$, as the degree is additive. Tensoring with $\mathcal{L}$ we get the exact sequence of vector bundles over C

$$0 \longrightarrow \mathcal{I} \otimes \mathcal{L} \longrightarrow \mathcal{F}_r^{\otimes n} \otimes \mathcal{L} \longrightarrow S^n(\mathcal{F}_r) \otimes \mathcal{L} \longrightarrow 0$$

and the exact cohomology sequence

$$0 \longrightarrow H^0(\mathcal{I} \otimes \mathcal{L}) \longrightarrow H^0(\mathcal{F}_r^{\otimes n} \otimes \mathcal{L}) \longrightarrow H^0(S^n(\mathcal{F}_r) \otimes \mathcal{L}) \longrightarrow$$

$$H^1(\mathcal{I} \otimes \mathcal{L}) \longrightarrow H^1(\mathcal{F}_r^{\otimes n} \otimes \mathcal{L}) \longrightarrow H^1(S^n(\mathcal{F}_r) \otimes \mathcal{L}) \longrightarrow 0.$$

The higher degree terms vanish by the Grothendieck vanishing theorem cited at page 52. We know by case (6) of Theorem 6.11 that $h^0(\mathcal{F}_r^{\otimes n} \otimes \mathcal{L}) = 0$, so, by the Riemann-Roch theorem, we obtain

$$h^1(\mathcal{F}_r^{\otimes n} \otimes \mathcal{L}) = h^0(\mathcal{F}_r^{\otimes n} \otimes \mathcal{L}) - \deg(\mathcal{F}_r^{\otimes n} \otimes \mathcal{L}) = 0 \ .$$

This way the cohomology sequence becomes

$$0 \longrightarrow H^0(\mathcal{I} \otimes \mathcal{L}) \longrightarrow 0 \longrightarrow H^0(S^n(\mathcal{F}_r) \otimes \mathcal{L}) \longrightarrow$$

$$H^1(\mathcal{I} \otimes \mathcal{L}) \longrightarrow 0 \longrightarrow H^1(S^n(\mathcal{F}_r) \otimes \mathcal{L}) \longrightarrow 0.$$

Thus $H^0(\mathcal{I} \otimes \mathcal{L}) = 0$ and, by the Riemann-Roch theorem, $H^1(\mathcal{I} \otimes \mathcal{L}) = 0$. Therefore we get the exact sequence

$$0 \longrightarrow H^0(S^n(\mathcal{F}_r) \otimes \mathcal{L}) \longrightarrow 0 \ ,$$

then it turns out that $H^0(S^n(\mathcal{F}_r) \otimes \mathcal{L}) = 0$, so $\deg \mathcal{E}_i \leq 0$ for every i. Since the degree is additive over direct sums, $\deg \mathcal{E}_i = 0$ for every i. From Theorem 6.11, $\mathcal{E}_i \cong \mathcal{F}_{r_i} \otimes \mathcal{L}_i$ for some degree 0 line bundles $\mathcal{L}_i$. We want to prove that $\mathcal{L}_i \cong \mathcal{O}_C$ for all i. Assume $\mathcal{L}_i \ncong \mathcal{O}_C$ for some i. We can tensor with $\mathcal{L}_i^{-1}$ and so we obtain the cohomology sequence

$$0 \longrightarrow H^0(\mathcal{I} \otimes \mathcal{L}^{-1}) \longrightarrow H^0(\mathcal{F}_r^{\otimes n} \otimes \mathcal{L}^{-1}) \longrightarrow H^0(S^n(\mathcal{F}_r) \otimes \mathcal{L}^{-1}) \longrightarrow$$

$$H^1(\mathcal{I} \otimes \mathcal{L}^{-1}) \longrightarrow H^1(\mathcal{F}_r^{\otimes n} \otimes \mathcal{L}^{-1}) \longrightarrow H^1(S^n(\mathcal{F}_r) \otimes \mathcal{L}^{-1}) \longrightarrow 0.$$

Arguing analogously to what we did before we can show that in this case $H^0(S^n(\mathcal{F}_r) \otimes \mathcal{L}^{-1}) = 0$. But $S^n(\mathcal{F}_r) \otimes \mathcal{L}^{-1}$ has $\mathcal{F}_{r_i}$ as a direct summand, so it has no zero global sections and this contradicts the assumption $\mathcal{L}_i \ncong \mathcal{O}_C$ for some i. Hence we found $S^n(\mathcal{F}_r) \cong \bigoplus_i \mathcal{F}_{r_i}$. The rank computation follows easily from Theorem 6.8. □

The last step is given by the following theorem, proved by Atiyah for algebraically closed fields of characteristic 0, whose generalization to perfect fields is possible by [11]. A proof can be found in [23, appendix A p.20].

Theorem 6.12 *Let C be an elliptic curve. Then every indecomposable vector bundle over C is semistable.*

By Theorem 6.12 and Proposition 6.9 we can for the first time explicitly calculate the parameters of some codes constructed on surfaces.

Theorem 6.13 *Let C be an elliptic curve with γ $\mathbf{F}_q$-rational points. Let a, b be integers with $0 < b < \gamma$, $0 \leq a < q+1$. Then there are $[n, d, k]$-codes with*

$$n = (q+1)\gamma$$

$$\mathrm{k} = (a+1)b$$

$$d \geq (q+1-a)(\gamma - b).$$

Proof: Take a normalized indecomposable degree zero rank 2 vector bundle $\mathcal{E}$ on C and apply Theorem 6.3. $\mathcal{E}$ is not ample because an indecomposable vector bundle on C is ample if and only if $\deg \mathcal{E} > 0$ ([8, cor. 7.7]), so in Theorem 6.3 we get $m = b$. We have just to calculate the dimension of the code. We obtain

$$h^0(C, S^a(\mathcal{E}) \otimes \mathcal{O}_C(bP_0)) = h^0(C, \bigoplus (\mathcal{F}_{r_i} \otimes \mathcal{O}_C(bP_0))) =$$

$$= \sum h^0(C, \mathcal{F}_{r_i} \otimes \mathcal{O}_C(bP_0)).$$

But $\mathcal{F}_{r_i}$ are semistable, so $\mathcal{F}_{r_i} \otimes \mathcal{O}_C(bP_0)$ are semistable and

$$\deg(\mathcal{F}_{r_i} \otimes \mathcal{O}_C(bP_0)) = r_i b > 0 \ ,$$

so $H^1(\mathcal{F}_{r_i} \otimes \mathcal{O}_C(bP_0)) = 0$. By the Weil-Riemann-Roch theorem cited at page 67, $h^0(\mathcal{F}_{r_i} \otimes \mathcal{O}_C(bP_0)) = r_i b$. We finally can write

$$\mathrm{k} = \sum h^0(C, \mathcal{F}_{r_i} \otimes \mathcal{O}_C(bP_0)) = b \sum r_i = b(a+1) \ .\square$$

REMARK: Lomont's proof of Theorem 6.13 is not completely clear. He writes that $h^0(C, \mathcal{F}_r \otimes \mathcal{O}_C(bP_0)) = 0$ comes from the Riemann-Roch theorem, as stated in [7]. But in Hartshorne's book the Riemann-Roch theorem is proved just for line bundles, while $\mathcal{F}_{r_i}$ has rank not necessarily 1.

Let us consider now the indecomposable rank 2 vector bundle with $\deg \mathcal{E} = 1$. We know that if $\mathcal{L}$ is a line bundle of degree 1, then $\deg(\mathcal{E} \otimes \mathcal{L}) = 3 > 2 = \mathrm{rank}\,(\mathcal{E} \otimes \mathcal{L})(2g-1)$. Hence $\mathcal{E}(1)$ is generated by global sections by Proposition 6.9. We can apply the case (2) of Theorem 6.10. By [8, cor. 7.7] $\mathcal{E}$ is ample so $m = b - ae = b + a$.

$\bar{\mathbf{R}}$	**a**	**b**	**rate**	δ	**a**	**b**	**rate**	δ
0.1	82	79	0.100053	0.100252	72	54	0.469978	0.364157
0.2	115	113	0.200015	0.200015	112	60	0.307683	0.183642
0.3	141	139	0.301183	0.300114	148	58	0.205325	0.0814984
0.4	163	160	0.400397	0.400092	183	51	0.136263	0.0237125

Table 3: Comparison between the degree 0 and the degree 1 case.

Theorem 6.14 (Zampolini) *Let C be an elliptic curve with γ $\mathbb{F}_q$-rational points. Let a, b be integers with $0 < b < \gamma$, $0 \leq a < q+1$. Then there are $[n, d, k]$-codes with*

$$n = (q+1)\gamma$$

$$\mathrm{k} \geq (a+1)(b + \frac{a}{2})$$

$$d \geq (q+1-a)(\gamma - a - b) \ .$$

Moreover, if $b > a$ then $\mathrm{k} = (a+1)(b+\frac{a}{2})$.

REMARK: For arbitrary a and b we were not able to calculate the dimension this way. In fact, if $b \leq a$ it is not possible to apply Proposition 6.9. In this case $h^1((C, S^a(\mathcal{E}) \otimes \mathcal{O}_C(bP_0))$ can be positive and so $\mathrm{k} > (a+1)(b+\frac{a}{2})$.

We wish to compare in one example the codes obtained in degree 0 case (Theorem 6.13) and the ones in degree 1 case (Theorem 6.14). In the second case we cannot always estimate the dimension, so we use just the lower bound. Consider the elliptic curve $y^2z = x^3 + xz + z^3$ over $\mathbb{F}_{256}$, which has $\gamma = 256$ rational points. The comparison method is the same as the one used at page 65. On the left side of the table we write the values in the degree 0 case, while on the right part we write the degree 1 case. We show the values for $\bar{R}$ up to 0.4, as the lower bound for the dimension does not ensure the existence with the desired rate for $\bar{R}$ greater or equal 0.5.
The table clearly shows that the codes from the 0 degree case are much more efficient than the codes from the 1 degree case. This is probably because we are not able to calculate their exact dimension for every a and b, but we know just a lower bound and the value for $b > a$. Moreover, remark that, even considering the bound, the best codes have $b > a$, so we still have a chance to increase the dimension of the first cohomolgy group of $S^a(\mathcal{E}) \otimes \mathcal{O}_C(bP_0)$.

The next proposition uses the same technique of Theorem 6.14 to prove a more general version of it. We write this formulation to emphasize the connection between $h^0(S^a(\mathcal{E}) \otimes \mathcal{O}_C(bP_0))$ and the indecomposable components of $S^a(\mathcal{E})$.

Proposition 6.11 *Let $\mathcal{E}$ be a vector bundle of rank 2 and degree $-e$ over an elliptic curve. Write $S^a(\mathcal{E}) = \bigoplus \mathcal{E}_\rangle$ with $\mathcal{E}_\rangle$ indecomposable,* $\deg \mathcal{E}_i = d_i$ *and* $\operatorname{rank} \mathcal{E}_i = r_i$*. Then*

$$h^0(S^a(\mathcal{E}) \otimes \mathcal{O}_C(bP_0)) = (a+1)(b - \frac{ea}{2}) + \sum_j h^1(C, \mathcal{E}_j \otimes \mathcal{O}_C(bP_0)),$$

where the sum is over j such that $d_j \leq -br_j$.

Proof: By Theorem 6.6,

$$h^0(S^a(\mathcal{E}) \otimes \mathcal{O}_C(bP_0)) = \deg(S^a(\mathcal{E}) \otimes \mathcal{O}_C(bP_0)) + h^1(S^a(\mathcal{E}) \otimes \mathcal{O}_C(bP_0)) =$$

$$= (b - \frac{ea}{2}) + h^1(S^a(\mathcal{E}) \otimes \mathcal{O}_C(bP_0)).$$

But

$$h^1(S^a(\mathcal{E}) \otimes \mathcal{O}_C(bP_0)) = \sum h^1(C, \mathcal{E}_i \otimes \mathcal{O}_C(bP_0)).$$

Remarking that $\deg(\mathcal{E}_i \otimes \mathcal{O}_C(bP_0)) = d_i + br_i$ and $\operatorname{rank}(\mathcal{E}_i \otimes \mathcal{O}_C(bP_0)) = r_i$ we have, since the $\mathcal{E}_i$ are semistable, that, if $d_j + br_j > r_j$ then, $h^1(\mathcal{E}_i \otimes \mathcal{O}_C(bP_0)) = 0$ by Proposition 6.9. □

6.8 Conclusion and open problems

As the study of codes on higher dimensional varieties is quite recent, many problems remain open and many "territories" are still left almost untouched by research.

The first natural question is if it is possible to study the properties of codes built on varieties of dimension bigger than 2. A first trial could probably be done for $\mathbb{P}^n$.

About codes on surfaces, one can try to calculate the parameters of codes on surfaces different from ruled surfaces. The only paper we know oriented in that direction is [6].

We saw that the classification of codes on rational ruled surfaces is completed, while for elliptic curves the case of vector bundles $\mathcal{E}$ of degree 1 is partially uncompleted. We calculated $h^0(S^a(\mathcal{E}) \otimes \mathcal{O}_C(bP_0))$ for $b > a$ and we emphasized how in general the solution of the problem is related to the knowledge of the indecomposable components of $S^a(\mathcal{E})$. Nevertheless, if we were able to compute the obstruction $h^1(S^a(\mathcal{E}) \otimes \mathcal{O}_C(bP_0))$ for $a \leq b$, we could build codes with better parameters. We suggest that probably it can be useful to solve the problem not for every indecomposable rank 2 vector bundle, but just for the only normalized one (see [7]).

Clearly it can be interesting to classify codes on ruled surface over curves of genus greater than 1, for example over hyperelliptic curves. A deep knowledge about vector bundles over them is required, so we suggest [3].

A fundamental problem to use AG codes on surfaces in the applications is the absence of a fast decoding algorithm. Zarzar and Voloch proposed an algorithm in [27], but, by now, we have no proof that it works for every code. One can either try to prove that Zarzar and Voloch's algorithm is able to decode at least codes on ruled surfaces or to look for a new algorithm for codes on ruled surfaces.

As a final remark, we mention an interesting paper by T. Johnsen ([12]), which connects rank 2 vector bundles over curves and the decoding of AG codes on curves. By this work, the study on rank 2 vector bundle over curves can be useful to develop both the theory of AG codes on ruled surface and the research of faster decoding algorithms for AG codes on curves.

References

[1] M.F. Atiyah. Vector bundles over an elliptic curve. *Proc. London Math. Soc.*, 7:414–457, 1957.

[2] E. Bombieri [d'aprés Stefanov]. Counting points on curves over finite fields. *Sem. Bourbaki*, 25:234–241, 1972/73.

[3] U.V Desale and S. Ramanan. Classification of vector bundles of rank 2 on hyperelliptic curves. *Inventiones Mathematicae*, 38:161–185, 1976.

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

[5] D. Gieseker. Stable vector bundles and the frobenius morphism. *Anneles scientifiques de l' E.N.S*, 6:95–101, 1973.

[6] S.H. Hansen. *Error-Correcting Codes from higher-dimensional varieties*. PhD thesis, University of Aarhus, 2001.

[7] R. Harsthorne. *Algebraic geometry*. Springer- Verlag, 1977.

[8] R. Hartshorne. Ample vector bundles. *Publications matheematiques de l'I.H.E.S*, 26:63–94, 1966.

[9] R. Hartshorne. *Ample subvarieties of algebraic varieties*. Springer Verlag, 1970.

[10] Y. Ihara. Some remarks on the number of rational points on algebraic curves over finite fields. *J. Fac. Sci. Univ. Tokyo Sect. IA Math*, 28:721–724, 1981.

[11] R. Elman J.K. Arason and B. Jacob. On indecomposable vector bundles. *Comm. Algebra*, 20:1323–1351, 1992.

[12] T. Johnsen. Rank two bundles on algebraic curves and decoding of Goppa codes. *Int. J. Pure Appl. Math.*, 4:33–35, 2003.

[13] G.R. Kempf. *Algebraic Varieties*. Cambridge University Press, 1993.

[14] S. Lang. *Algebra*. Addison-Wesley, 1971.

[15] Q. Liu. *Algebraic Geometry and Arithmetic Curves*. Oxford University Press, 2002.

[16] C. Lomont. *Error correcting codes on algebraic surfaces*. PhD thesis, Purdue University, 2003.

[17] Yu. Manin and S.G. Vladut. Linear codes and modular curves. *J. Soviet Math.*, 30:2611–2642, 1985.

[18] C. Munera and R. Pellikaan. Self-dual and decomposable geometric goppa codes. *Eurocode*, 92:77–87, 1993.

[19] O. Pretzel. *Codes and algebraic curves*. Clarendon Press, 1998.

[20] C.E. Shannon. A mathematical theory of communication. *Bell Sys. Tech. J.*, 27:379–423, 1948.

[21] M.A. Tsfasman and S.G. Vladut. *Algebraic-Geometric codes*. Kluwer Academic Publisher, 1991.

[22] M.A. Tsfasman, S.G. Vladut, and T. Zink. Modular curves, Shimura curves, and Goppa codes better than the Varshamov-Gilbert bound. *Math. Nachrichten*, 109:21–28, 1982.

[23] L.W. Tu. Semistable bundles over an elliptic curve. *Advances in Mathematics*, (98):1–26, 1993.

[24] G. van der Geer and J.H van Lint. *Introduction to Coding Theory and Algebraic Geometry*. Birkhauser, 1988.

[25] J.H. van Lint. *Introduction to Coding Theory*. Springer, 1998.

[26] S.G. Vladut and V.G. Drinfeld. Number of points of an algebraic curve. *Functional Anal. Appl.*, 17:53–54, 1983.

[27] J.F. Voloch and M. Zarzar. Algebraic geometric codes on surfaces. *submitted to Proceeding of A.G.C.T. 10*, 2005.