Differential Approach for the Study of Duals of Algebraic-Geometric Codes on Surfaces

Alain Couvreur

DIFFERENTIAL APPROACH FOR THE STUDY OF DUALS OF ALGEBRAIC-GEOMETRIC CODES ON SURFACES

ALAIN COUVREUR

ABSTRACT. The purpose of the present article is the study of duals of functional codes on algebraic surfaces. We give a direct geometrical description of them, using differentials. Even if this geometrical description is less trivial, it can be regarded as a natural extension to surfaces of the result asserting that the dual of a functional code $C_L(D, G)$ on a curve is the differential code $C_\Omega(D, G)$. We study the parameters of such codes and state a lower bound for their minimum distance. Using this bound, one can study some examples of codes on surfaces, and in particular surfaces with Picard number 1 like elliptic quadrics or some particular cubic surfaces. The parameters of some of the studied codes reach those of the best known codes up to now.

INTRODUCTION

Given a variety X over a finite field, a divisor G on X and a family $P_1, \ldots, P_n$ of rational points of X, one can construct the *functional code* $C_L(X, \Delta, G)$, where Δ denotes the formal sum $P_1 + \cdots + P_n$. This construction, due to Manin in [22], is obtained by evaluating the global sections of the sheaf $\mathcal{L}(G)$ at the points $P_1, \ldots, P_n$. Basically, the aim of this paper is to get information on the dual $C_L(X, \Delta, G)^\perp$ of such a functional code.

Most of the literature on algebraic–geometric codes deals with the case when X is a curve. In this situation, the dual code $C_L(X, \Delta, G)^\perp$ is equal to the *differential* code $C_\Omega(X, \Delta, G)$ whose construction, due to Goppa in [9], involves residues of differential forms on X. Moreover, on curves, it is also well-known that a differential code $C_\Omega(X, \Delta, G)$ is equal to a functional code $C_L(X, \Delta, G')$, where G' is a divisor depending on G, Δ and the canonical class of X. Therefore, the study of duals of functional codes on curves is equivalent to the study of functional codes.

For higher–dimensional varieties, the geometric problems raised by coding theory become much more difficult and hence only little is known. Most of the literature on the topic concerns the estimation of the parameters and in particular the minimum distance of functional codes on particular surfaces. For instance, codes on quadric varieties are studied in [1] and [7], codes on surfaces with Picard number 1 are studied in [24] (see the survey chapter of J.B. Little in [14] for a detailed survey on the topic). Concerning the dual of such a functional code, almost nothing is known. In [3], a differential construction for codes on surfaces is given, which turns out to be a natural extension to surfaces of Goppa's construction on curves (see [9]). It is proved in the same article that such a differential code is contained in the dual of a functional code, but that the converse inclusion is false in general.

The aim of the present paper is to get general information on duals of functional codes on surfaces. For that, we try to answer two questions asked in

Section 3. The first one (which was actually raised in the end of [3]) is to find a direct geometrical description of such a code using differentials. The second one is to get information on the parameters of such codes. As an answer for the first question, we state and prove Theorem 5.1. This statement asserts that even if the dual of a functional code on a surface is not differential in general, it is always a sum of differential codes on this surface. Afterwards, we focus our study on the estimate of the parameters of such a code and state results yielding a lower bound for its minimum distance. When the surface is the projective plane, these results yield the exact minimum distance which is already known in this case since the codes are Reed–Muller (see [5] Theorem 2.6.1). In addition, these results (Theorems 6.4 and 6.6) are easy to handle provided the Picard number of the surface is small. It is worth noting that the works on parameters of codes on surfaces point out that surfaces with Picard number 1 yield good functional codes. This principle was first observed by Zarzar in [24] and is confirmed by some other works on the topic. For instance, one sees in [7] that elliptic quadrics (which have Picard number 1) give much better codes than hyperbolic ones (which have Picard number 2). It turns out that this principle asserting that surfaces with small Picard number yield good functional codes seems to hold for duals of functional codes. Two examples of surfaces with Picard number 1 are studied (namely, elliptic quadrics and cubic which do not contain rational lines). The minimum distance of some dual codes obtained from these examples turn out to reach the best known minimum distance up to now compared to their length and dimension.

Contents. Notations are given in Section 1. They are followed by the recall of some prerequisites in Section 2. The aims of the present article are summarised in Section 3, where Questions 1 and 2 are raised. Section 4 is devoted to the proof of some statements which are important in what follows. In particular, Proposition 4.9, which is the key tool for the proof of the two main results (Theorems 5.1 and 6.4), is proved in this section. Section 5 is devoted to the answer to Question 1. Theorem 5.1 is proved in this section and asserts that, even if the dual of a functional code on a surface is not in general a differential code on this surface, it is always a sum of differential codes on this surface. Section 6 is devoted to the answer to Question 2, that is the study of the minimum distance of the dual of a functional code on a surface. Two results are stated: Theorem 6.4, yielding a lower bound for the minimum distance of some of these codes, and Theorem 6.6, which improves the bound given by Theorem 6.4 in some situations. Some applications of Theorems 6.4 and 6.6 are studied in Section 7, and lower bounds for the minimum distance are given for explicit examples. The parameters of these codes are compared with those of the best known codes up to now (found in [10] and [18]).

1. Notations

1.1. **About coding theory.** An error–correcting code is a vector subspace C of $\mathbf{F}_q^n$ for some positive integer n. The integer n is called the *length* of C. Elements of C are called *codewords*. The *Hamming weight* $w(c)$ of a vector $c \in \mathbf{F}_q^n$ is the number of its nonzero coordinates. The *Hamming distance* $d(x, y)$ between two vectors $x, y \in \mathbf{F}_q^n$ is $d(x, y) := w(x - y)$. Given a code $C \in \mathbf{F}_q^n$, the *minimum distance* d of C is the smallest Hamming distance between two distinct elements

of C. A code is said to have parameters $[n, k, d]$ if its length is n, its dimension over $\mathbf{F}_q$ is k and its minimum distance is d.

On $\mathbf{F}_q^n$, we consider the canonical pairing $\langle ., . \rangle$ defined by $\langle x, y \rangle := \sum_{i=1}^n x_i y_i$. Given a code $C \subset \mathbf{F}_q^n$, its orthogonal space $C^\perp$ for this pairing is called *dual code* of C.

1.2. About divisors and sheaves.

Given a sheaf $\mathcal{F}$ on a variety X, we denote by $\mathcal{F}_P$ its stalk at a point $P \in X$. Linear equivalence between divisors is denoted by $D \sim D'$. Given a map $\nu : Y \hookrightarrow X$ between two varieties and a divisor G on X, then, for convenience's sake, the pullback $\nu^\star G$ is denoted by $G^\star$ whenever there is no possible confusion on ν. Given a projective variety V, we denote by H_V the hyperplane section of V and by K_V its canonical class.

1.3. About intersections.

Let S be an algebraic surface, P be a smooth point of S and X, Y be two curves embedded in S. If X and Y have no common irreducible component in a neighbourhood of P, we denote by $m_P(X, Y)$ the intersection multiplicity of X and Y at P. The notion of intersection multiplicity extends by linearity to divisors on S. Finally, the intersection product of two divisor classes D and D' is denoted by $D.D'$.

1.4. Base field extensions.

Let X be a variety defined over $\mathbf{F}_q$. We denote by $\overline{X}$ the variety $\overline{X} := X \times_{\mathbf{F}_q} \overline{\mathbf{F}}_q$. In the same way, let $\mathcal{F}$ be a sheaf on X, then we denote by $\overline{\mathcal{F}}$ the pullback of $\mathcal{F}$ on $\overline{X}$.

2. Prerequisites

In this section we recall some facts about residues and differential forms on surfaces. Afterwards, we give some necessary prerequisites on algebraic–geometric codes on surfaces.

2.1. Residues of differential 2-forms on algebraic surfaces.

For further details on the definitions and the statements given in the present subsection, see [3] and [4]. Some results on residues can also be found in [15].

2.1.1. *Residues in codimension* 1. Let C be an irreducible curve embedded in a smooth surface S over an arbitrary field k. If ω is a differential 2–form on S with valuation ≥ -1 along C, then one can define a 1–form on C denoted by $\mathrm{res}_C^1(\omega)$. See [3] Definition 1.3.

2.1.2. *Residues in codimension* 2. Let C be an irreducible curve embedded in a surface S and P be a rational point of S. Given a 2-form ω on S, one defines a residue at P along C of ω denoted by $\mathrm{res}_{C,P}^2(\omega)$ (see [3] Definition 3.1 and Theorem 3.6). By convention, the map $\mathrm{res}_{C,P}^2$ is identically zero when $P \notin C$. This notion generalises to any arbitrary reduced curve C. In this situation, $\mathrm{res}_{C,P}^2(\omega)$ is the sum of the residues of ω at P along each irreducible component of C. Finally, if D is a divisor on S, we denote by $\mathrm{res}_{D,P}^2$ the residue at P along the **reduced support** of D. That is $\mathrm{res}_{D,P}^2 := \mathrm{res}_{\mathrm{Supp}(D),P}^2$. The following proposition summarises the properties of 2–residues we need in what follows.

Proposition 2.1. *Let S be a smooth surface over an arbitrary field, D be a divisor on S and P be a rational point of S. Let ω be a rational 2–form on S.*

(i) *If in a neighbourhood of P, the pole locus of ω has no common component with $Supp(D)$, then $res^2_{D,P}(\omega) = 0$.*

(ii) *If in a neighbourhood of P, the pole locus of ω is entirely contained in $Supp(D)$, then $res^2_{D,P}(\omega) = 0$.*

In addition, let $C \subset S$ be a smooth curve at P.

(iii) *If ω has valuation ≥ -1 along C, then $res^2_{C,P}(\omega) = res_P(res^1_C(\omega))$.*

Proof. The definition of 2–residues ([3] Definition 3.1) gives (i). From [3] Theorem 6.3, we get (ii). Finally (iii) is a consequence of [3] Definitions 1.4 and 3.1 together with Remark 3.3. $\qquad\square$

Remark 2.2. Basically, Proposition 2.1 asserts that $res^2_{D,P}(\omega)$ is nonzero if and only if in any neighbourhood of P, the support of D contains at least one component of the pole locus of ω but does not contain entirely this pole locus. It entails in particular that nonzero residues appear only at points P at which two distinct poles of ω meet.

2.2. **Algebraic–geometric codes on surfaces.**

2.2.1. *Context.* Let S be a smooth projective geometrically connected surface over a finite field $\mathbf{F}_q$, let G be a divisor on S and $P_1, \ldots, P_n$ be a family of rational points of S avoiding the support of G. Denote by Δ the 0–cycle $\Delta := P_1 + \cdots + P_n$.

2.2.2. *Functional codes.* Recall the definition, due to Manin in [22], of the functional code associated to G and Δ. This code is defined to be the image of the evaluation map

$$ev_\Delta : \begin{cases} H^0(S, \mathcal{L}(G)) & \longrightarrow & \mathbf{F}_q^n \\ f & \longmapsto & (f(P_1), \ldots, f(P_n)). \end{cases}$$

It is denoted by $C_L(S, \Delta, G)$ or $C_L(\Delta, G)$ if there is no possible confusion on the involved variety.

2.2.3. *Differential codes.* A differential construction of codes on surfaces is given in [3] 8.1. Let D_a, D_b be two divisors on S whose supports have no common component, the differential code associated to Δ, D_a, D_b and G is the image of the map

$$res^2_{D_a,\Delta} : \begin{cases} H^0(S, \Omega^2(G - D_a - D_b)) & \longrightarrow & \mathbf{F}_q^n \\ \omega & \longmapsto & (res^2_{D_a,P_1}(\omega), \ldots, res^2_{D_a,P_n}(\omega)). \end{cases}$$

It is denoted by $C_\Omega(S, \Delta, D_a, D_b, G)$ or $C_\Omega(\Delta, D_a, D_b, G)$ when there is no possible confusion on the involved surface.

If there is no relation between the pair (D_a, D_b) and Δ, then there is no interesting relation between $C_L(S, \Delta, G)$ and $C_\Omega(S, \Delta, D_a, D_b, G)$. This motivates the notion of Δ–convenient pair of divisors.

Definition 2.3 (Δ–convenience, [3] Definition 8.3)**.** A pair (D_a, D_b) is said to be Δ–convenient if

(i) the supports of D_a and D_b have no common irreducible component;
(ii) for all $P \in \overline{S}$, the map $res^2_{D_a,P} : \overline{\Omega^2(-D_a - D_b)}_P \to \overline{\mathbf{F}}_q$ is $\mathcal{O}_{\overline{S},P}$–linear;
(iii) this map is surjective for all $P \in \mathrm{Supp}(\Delta)$ and zero elsewhere.

Remark 2.4. Some examples and pictures illustrating this notion are given in [4] II.3.4 and 5. An explicit criterion for Δ–convenience involving intersection multiplicities is given in [3] Proposition 8.6.

In what follows, we also use a weaker definition called *sub–Δ–convenience.*

Definition 2.5 (Sub–Δ–convenience, [4] III.2.1)**.** A pair (D_a, D_b) is said to be sub–Δ–convenient if it is Δ'–convenient for some $0 \leq \Delta' \leq \Delta$. Equivalently, the pair satisfies the conditions (i) and (ii) of the previous definition together with

(iii') for all $P \in \overline{S} \smallsetminus \mathrm{Supp}(\Delta)$, the map $\mathrm{res}^2_{D_a, P} : \overline{\Omega^2(-D_a - D_b)}_P \to \overline{\mathbf{F}}_q$ is zero.

3. STATEMENT OF THE PROBLEMS

On a curve X with a divisor G and a sum of rational points D (which is also a divisor), it is well-known that the dual of the functional code $C_L(X, D, G)$ equals the differential code $C_\Omega(X, D, G)$ (for instance see [20] II.2.8). On a surface S with a divisor G and a sum of rational points Δ (which is not a divisor!), the situation is not that simple. Nevertheless, it has been proved in [3] Theorem 9.1, that, if (D_a, D_b) is a Δ–convenient pair, then $C_\Omega(S, \Delta, D_a, D_b, G) \subseteq C_L(S, \Delta, G)^\perp$.

Remark 3.1. This holds for a sub–Δ–convenient pair (with the very same proof).

As said in the introduction, the reverse inclusion is in general false. This motivates the following questions (the first one is raised in the end of [3]).

Question 1. *Can the code $C_L(S, \Delta, G)^\perp$ be realised as a sum of differential codes on S associated to different pairs of (sub–)Δ–convenient divisors?*

Question 1b. *Given $c \in C_L(S, \Delta, G)^\perp$, does there exist a (sub–)Δ–convenient pair (D_a, D_b) such that $c \in C_\Omega(S, \Delta, D_a, D_b, G)$?*

Question 2. *How can one estimate or find a lower bound for the minimum distance of the code $C_L(S, \Delta, G)^\perp$?*

Theorem 5.1 answers positively to Question 1b, which entails a positive answer for Question 1 (see Corollary 5.3). Theorems 6.4 and 6.6 yield a method to estimate the minimum distance of duals of functional codes.

Remark 3.2. Actually, it is proved in [4] §III.3 that Questions 1 and 1b are equivalent. However, such a proof is not necessary in what follows.

4. THE MAIN TOOLS

The present section contains some tools which are needed to prove the main results of this article (Theorems 5.1 and 6.4). In particular, Proposition 4.9, which is the key tool of this paper is proved here.

The reader interested in the results and their applications can skip this section in a first reading and look at the applications in Sections 5 and 6.

4.1. **A problem of interpolation.** The proofs of Proposition 4.9 and Theorem 5.1 need some result due to Poonen in [17] Theorem 1.2. To state this result, we need to introduce some notations and definitions.

Notation 4.1. For all integers $d, r \geq 0$, we denote by $S_{d,r}$ the subspace of $\mathbf{F}_q[X_0, \ldots, X_r]$ of homogeneous polynomials of degree d. We denote then by S_r the set $S_r := \cup_{d \geq 0} S_{d,r}$.

Definition 4.2 (Poonen, [17] §1). The density $\mu(\mathcal{P})$ of a part $\mathcal{P}$ of S_r is defined by

$$\mu(\mathcal{P}) := \lim_{d \to +\infty} \frac{\sharp(\mathcal{P} \cap S_{d,r})}{\sharp S_{d,r}}.$$

Theorem 4.3 (Poonen, [17] 1.2). *Let X be a quasi-projective sub scheme of $\mathbf{P}^r$ over $\mathbf{F}_q$. Let Z be a finite sub-scheme of $\mathbf{P}^r$, and assume that $U := X \setminus (Z \cap X)$ is smooth of dimension $m \geq 0$. Fix a subset $T \subseteq H^0(Z, \mathcal{O}_Z)$. Given $f \in S_{d,r}$, let $f_{|Z}$ be the element of $H^0(Z, \mathcal{O}_Z)$ that on each connected component Z_i equals the restriction of $X_j^{-d} f$ to Z_i, where $j = j(i)$ equals the smallest $j \in \{0, \ldots, n\}$ such that the coordinate X_j is invertible on Z_i. Define*

$$\mathcal{P} := \{f \in S_r : \ \{f = 0\} \cap U \text{ is smooth of dimension } m - 1, \text{ and } f_{|Z} \in T\}.$$

Then,

$$\mu(\mathcal{P}) = \frac{\sharp T}{\sharp H^0(Z, \mathcal{O}_Z)} \zeta_U(m+1)^{-1},$$

where $\zeta_U(s) = Z_U(q^{-s})$ denotes the Zeta function of U.

Corollary 4.4. *Let S be a smooth projective surface over $\mathbf{F}_q$ and $Q_1, \ldots, Q_s$ be a finite set of rational points of S. There exists an integer $s \geq 0$ such that for all $d \geq s$, there exists a hypersurface H of degree d in $\mathbf{P}^r$ whose scheme–theoretic intersection with S is smooth of codimension 1 and contains $Q_1, \ldots, Q_s$.*

Proof. For $j \in \{1, \ldots, s\}$ denote by $\mathcal{I}_j$ the sheaf of ideals of $\mathcal{O}_X$ corresponding to Q_j. Let $\mathcal{I}$ be the sheaf of ideals $\mathcal{I} := \mathcal{I}_1 \cdots \mathcal{I}_s$. Denote by Z the non-reduced sub-scheme of X defined by the finite set $\{Q_1, \ldots, Q_s\}$ with the structure sheaf $\mathcal{O}_Z := \mathcal{O}_S/\mathcal{I}^2$. Let T be the set

$$T := \left\{f \in H^0(Z, \mathcal{O}_Z) | \ \forall j, \ f \in H^0(Z, \mathcal{I}_j \mathcal{O}_Z) \setminus \{0\}\right\}.$$

For all $n \in \mathbf{N}$ and all $f \in H^0(X, \mathcal{O}_X(n))$, $f_{|Z} \in T$ means that the vanishing locus of f on X contains all the Q_i's and is smooth at each of them. We conclude by applying Theorem 4.3. $\qquad\square$

4.2. **A vanishing problem.** As we see further in 4.3, the statement of Proposition 4.9 expects a vanishing condition on the sheaf cohomology space $H^1(S, \Omega^2(G - X))$, where S is a smooth projective surface and G, X are divisors on S. The point of the present section is to give some criteria on G and X to satisfy such a vanishing condition.

Lemma 4.5. *Let S be a smooth projective geometrically connected surface over a field k, G be an arbitrary divisor on S and L be an ample divisor. Then, there exists an integer m such that for all $s \geq m$, we have*

$$H^1(S, \mathcal{L}(G - sL)) = H^1(S, \Omega^1(G - sL)) = 0.$$

Proof. From [11] Corollary III.7.8, the space $H^1(S, \mathcal{L}(G - sL))$ is zero for all $s \gg 0$. Since S is assumed to be smooth, Serre's duality yields the other equality. $\quad\square$

Lemma 4.6. *Let S be a smooth projective geometrically connected surface over a field k which is a complete intersection in a projective space $\mathbf{P}_k^r$ for some $r \geq 3$. Denote by H_S the hyperplane section on S for this projective embedding. Let G be a divisor on S such that $G \sim mH_S$ for some integer m and $X \subset S$ be a curve which is a complete intersection in $\mathbf{P}^r$. Then,*

$$H^1(S, \mathcal{L}(G - X)) = H^1(S, \Omega^1(G - X)) = 0.$$

Proof. Consider the exact sequence of sheaves on S

$$0 \to \mathcal{L}(G - X) \to \mathcal{L}(G) \to i_\star \mathcal{L}(G^\star) \to 0,$$

where i denotes the canonical inclusion map $i : X \hookrightarrow S$. Looking at the long exact sequence in cohomology, we have

$$(1) \qquad H^0(S, \mathcal{L}(G)) \to H^0(X, \mathcal{L}(G^\star)) \to H^1(S, \mathcal{L}(G - X)) \to H^1(S, \mathcal{L}(G)).$$

Since $G \sim mH_S$, the sheaves $\mathcal{L}(G)$ on S and $\mathcal{L}(G^\star)$ on X are respectively isomorphic to $\mathcal{O}_S(m)$ and $\mathcal{O}_X(m)$. In addition, since S is a complete intersection in $\mathbf{P}^r$, we have $H^1(S, \mathcal{L}(G)) = H^1(S, \mathcal{O}_S(m)) = 0$ (see [11] Exercise III.5.5(c)). Thus (1) together with the above claims yield

$$(2) \qquad H^0(S, \mathcal{O}_S(m)) \to H^0(X, \mathcal{O}_X(m)) \to H^1(S, \mathcal{L}(G - X)) \to 0.$$

Moreover, from [11] Exercise III.5.5(a), the natural restriction map

$$H^0(\mathbf{P}^r, \mathcal{O}_{\mathbf{P}^r}(m)) \to H^0(X, \mathcal{O}_X(m))$$

is surjective. Since this map is the composition of

$$H^0(\mathbf{P}^r, \mathcal{O}_{\mathbf{P}^r}(m)) \to H^0(S, \mathcal{O}_S(m)) \quad \text{and} \quad H^0(S, \mathcal{O}_S(m)) \to H^0(X, \mathcal{O}_X(m)),$$

the right-hand map above is also surjective. The exact sequence (2) together with the previous assertion yield $H^1(S, \mathcal{L}(G - X)) = 0$. Finally, since S is smooth, Serre's duality entails $H^1(S, \Omega^2(G - X)) = 0$. $\qquad\qquad\square$

Remark 4.7. In Lemma 4.6, the curve X needs not to be a hypersurface section of S, one just expects it to be a complete intersection in the ambient space of S. For instance, Lemma 4.6 can be applied to a line X embedded in S.

4.3. **The key tool.** In the present subsection, we state Proposition 4.9, which is useful to prove Theorem 5.1 (answering Question 1b) and then to prove Theorem 6.4 (yielding lower bounds for the minimum distance of duals of functional codes on a surface).

In what follows we always stay in the context presented in 2.2.1.

Definition 4.8 (Support of a codeword)**.** In the context of 2.2.1, given a codeword c in $C_L(S, \Delta, G)$ or its dual, we call *support of c* and denote by $\mathrm{Supp}(c)$ the set of rational points $\{P_{i_1}, \ldots, P_{i_s}\}$ whose indexes correspond to the nonzero coordinates of c.

Proposition 4.9. *In the context of 2.2.1, let $c \in C_L(S, \Delta, G)^\perp$ be a nonzero codeword. Let X be a reduced curve embedded in S, containing the support of c and such that $H^1(S, \Omega^2(G - X)) = 0$. Then, there exists a divisor D on S such that*

(i) (D, X) is sub–Δ–convenient;
(ii) $c \in C_\Omega(S, D, X, G)$.

Moreover, if X is minimal for the property "X contains $\mathrm{Supp}(c)$" (i.e. any reduced curve $X' \subsetneq X$ avoids at least one $P \in \mathrm{Supp}(c)$), then

(iii) $w(c) \geq X.(G - K_S - X)$,

where K_S denotes the canonical class on S.

Remark 4.10. Since S is assumed to be smooth, by Serre's duality, the condition $H^1(S, \Omega^2(G - X)) = 0$ is equivalent to $H^1(S, \mathcal{L}(G - X)) = 0$.

The following lemma is needed in the proof of Proposition 4.9.

Lemma 4.11. *Let P be a point of S. Let $C \subset S$ be a smooth curve at P and $X, Y \subset S$ be two other curves such that any two of the curves C, X, Y have no common irreducible component in a neighbourhood of P. Then,*

$$m_P(X, Y) \geq \min\{m_P(C, X), m_P(C, Y)\}.$$

Proof. Let v be a local equation of C in a neighbourhood of P and let u be a rational function on S such that (u, v) is a system of local coordinates at P. Let $\phi_X, \phi_Y \in \mathcal{O}_{S,P}$ be respective local equations of X and Y in a neighbourhood of P. Denote by a_X and a_Y the respective P–adic valuations of the functions $\phi_{X|C}$ and $\phi_{Y|C}$ on the curve C.

Then, $m_P(C, X) = \dim \mathcal{O}_{S,P}/(\phi_X, v) = \dim \mathcal{O}_{C,P}/(\phi_{X|C}) = a_X$, and in the same way, $m_P(C, Y) = a_Y$. By symmetry, one can assume that $a_X \leq a_Y$. Then, let us prove that $1, u, \ldots, u^{a_X-1}$ are linearly independent in $\mathcal{O}_{S,P}/(\phi_X, \phi_Y)$. Let $\lambda_0, \ldots, \lambda_{a_X-1} \in \mathbf{F}_q$ such that

$$\lambda_0 + \lambda_1 u + \cdots + \lambda_{a_X-1} u^{a_X-1} = \alpha \phi_X + \beta \phi_Y,$$

for some $\alpha, \beta \in \mathcal{O}_{S,P}$. Reduce the above equality modulo v. This yields an equality in $\mathcal{O}_{C,P}$ whose right-hand term has (u)–adic valuation $\geq a_X$. Thus, $\lambda_0 = \cdots = \lambda_{a_X-1} = 0$. This concludes the proof. $\square$

Proof of Proposition 4.9. After a suitable reordering of the indexes, one can say that $\mathrm{Supp}(c) = \{P_1, \ldots, P_s\}$ for some $s \leq n$.

Step 0. Since S is projective, there exists a closed immersion $S \hookrightarrow \mathbf{P}^r$ for some $r \geq 3$. Let H_S be the corresponding hyperplane section.

Step 1. The curve C. From Corollary 4.4, there exists a curve $C \subset S$ such that

(1) C is smooth and geometrically connected;
(2) $C \not\subseteq X$;
(3) C contains $P_1, \ldots, P_s$;
(4) C is linearly equivalent to dH_S for some positive integer d.

Moreover, Corollary 4.4 asserts that d can be chosen to be as large as possible. Thus, from Lemma 4.5, choosing a large enough d, we have $H^1(S, \mathcal{L}(G - C)) = 0$ and hence

(4) the restriction map $H^0(S, \mathcal{L}(G)) \to H^0(C, \mathcal{L}(G^\star))$ is surjective.

Step 2. The codeword $c^\star$. Denote by F_c the divisor on C defined by

$$F_c := P_1 + \cdots + P_s \ \in \mathrm{Div}(C).$$

The surjectivity of the map $H^0(S, \mathcal{L}(G)) \to H^0(C, \mathcal{L}(G^\star))$, induces a natural code map $\phi : C_L(S, \Delta, G) \to C_L(C, F_c, G^\star)$ which is also surjective. It can be actually regarded as a puncturing map on the functional code on S (see [13] 1.9.(II) for a definition). Therefore, one sees easily that the orthogonal map $\phi^\perp : C_L(C, F_c, G^\star)^\perp \to C_L(S, \Delta, G)^\perp$

(a) is injective and obtained by extending codewords with $n - s$ zero coordinates on the right;
(b) preserves the Hamming distance;
(c) induces an isomorphism between $C_L(C, F_c, G^\star)^\perp$ and the sub-code of $C_L(S, \Delta, G)^\perp$ of codewords having their supports contained in $\{P_1, \ldots, P_s\}$.

Thus, c is in the image of $\phi^\perp$. Denote by $c^\star$ the codeword of $C_L(C, F_c, G^\star)^\perp$ such that $\phi^\perp(c^\star) = c$. It is the punctured codeword $(c_1, \ldots, c_s)$ of c obtained by removing all the zero coordinates. Obviously, we have $w(c) = w(c^\star)$.

Step 3. The 1–form μ. From [20] Theorem II.2.8, we have $C_L(C, F_c, G^\star)^\perp = C_\Omega(C, F_c, G^\star)$. Thus, since $c^\star \in C_L(C, F_c, G^\star)^\perp$, there exists a 1–form $\mu \in H^0(C, \Omega^1(G^\star - F_c))$ such that

$$c^\star = (\mathrm{res}_{P_1}(\mu), \ldots, \mathrm{res}_{P_s}(\mu)).$$

Step 4. The 2–form ω. As said in 2.1.1, any rational 2–form ν on S with valuation ≥ -1 along C has a 1–residue $\mathrm{res}_C^1(\nu)$ on C. This map res_C^1 is actually a surjective sheaf map, yielding the following exact sequence:

$$0 \to \Omega^2(G - X) \to \Omega^2(G - X - C) \overset{\mathrm{res}_C^1}{\longrightarrow} i_\star \Omega^1(G^\star - X^\star) \to 0,$$

where i denotes the canonical inclusion map $i : C \to S$. Using the corresponding long exact sequence in cohomology and since, by assumption, $H^1(S, \Omega^2(G - X))$ is zero, the map

$$(3) \qquad \mathrm{res}_C^1 : H^0(S, \Omega^2(G - X - C)) \to H^0(C, \Omega^1(G^\star - X^\star))$$

is surjective. Moreover, since X contains the points $P_1, \ldots, P_s$, we have the following divisors inequality on C:

$$0 \leq F_c \leq X^\star$$

and hence $H^0(C, \Omega^1(G^\star - F_c)) \subseteq H^0(C, \Omega^1(G^\star - X^\star))$. Thus, $\mu \in H^0(C, \Omega^1(G^\star - X^\star))$ and, since the map in (3) is surjective, there exists a 2–form $\omega \in H^0(S, \Omega^2(G - X - C))$ such that $\mu = \mathrm{res}_C^1(\omega)$.

Step 5. The divisor D. The divisor of ω is of the form

$$(4) \qquad (\omega) = G - X - C + A, \quad \text{with } A \geq 0.$$

Set

$$(5) \qquad D := C - A.$$

Step 6. Proof of (i). From the definition of sub–Δ–convenience (Definition 2.5), to prove the sub–Δ–convenience of (D, X), we have to prove that $\mathrm{res}_{D,P}^2$ is $\mathcal{O}_{\overline{S},P}$–linear for all $P \in \overline{S}$ and is zero whenever $P \notin \{P_1, \ldots, P_n\}$. Since the pole locus of ω is contained in $C \cup X$, from Proposition 2.1 and Remark 2.2, this map is zero at each $P \notin \overline{C} \cap \overline{X}$.

Moreover, recall that, by Definition of $\mathrm{res}_{D,P}^2$ (see §2.1.2), and from (5) we have $\mathrm{res}_{D,P}^2 = \mathrm{res}_{C,P}^2 + \mathrm{res}_{A,P}^2$ (by definition, the map depends only on the support D, thus it is an addition and not a subtraction). In addition, since any $\nu \in \overline{\Omega^2(-D - X)}_P$ has no pole along $\mathrm{Supp}(A)$, from Proposition 2.1(i), the map $\mathrm{res}_{A,P}^2$ vanishes on $\overline{\Omega^2(-D - X)}_P$ and hence

$$(6) \qquad \mathrm{res}_{D,P}^2 \equiv \mathrm{res}_{C,P}^2 \text{ on } \overline{\Omega^2(-D - X)}_P.$$

Thus, let us prove the $\mathcal{O}_{\overline{S},P}$–linearity of $\mathrm{res}_{C,P}^2$ at each $P \in \overline{C} \cap \overline{X}$ and prove that this map is zero if $P \notin \{P_1, \ldots, P_n\}$ (actually, we prove that this map is zero if and only if $P \notin \{P_1, \ldots, P_s\}$, which is stronger).

Let $P \in \overline{C} \cap \overline{X}$ and f be a generator of $\overline{\mathcal{L}(G)}_P$ over $\mathcal{O}_{\overline{S}, P}$. One sees easily that the germ of $f\omega$ generates $\overline{\Omega^2(-D-X)}_P$. Let $\varphi \in \mathcal{O}_{\overline{S}, P}$. From Proposition 2.1(iii), we have

$$(7) \qquad \mathrm{res}^2_{C,P}(\varphi f \omega) = \mathrm{res}_P(\mathrm{res}^1_C(\varphi f \omega)) = \mathrm{res}_P(\varphi_{|C} f_{|C} \mu).$$

Moreover, the divisor of $f_{|C}\mu$ satisfies $(f_{|C}\mu) \geq -F_c$ in a neighbourhood of P. Thus, if $P \in \{P_1, \dots, P_s\}$, then the 1–form $f_{|C}\mu$ has valuation -1 at P and

$$(7) \Rightarrow \mathrm{res}^2_{C,P}(\varphi f \omega) = \varphi(P)\mathrm{res}_P(f_{|C}\mu) = \varphi(P)\mathrm{res}^2_{C,P}(f\omega).$$

Otherwise, if $P \notin \{P_1, \dots, P_s\}$, then $f_{|C}\mu$ has valuation ≥ 0 at P and

$$(7) \Rightarrow \mathrm{res}^2_{C,P}(\varphi f \omega) = 0.$$

Thus, (D, X) is sub–Δ–convenient. It is actually Δ'–convenient for $\Delta' := P_1 + \dots + P_s$.

Step 7. Proof of (ii). From (6), we have for all $P \in \overline{S}$, $\mathrm{res}^2_{D,P}(\omega) = \mathrm{res}^2_{C,P}(\omega)$. Moreover, Proposition 2.1(iii) entails $\mathrm{res}^2_{C,P}(\omega) = \mathrm{res}_P(\mathrm{res}^1_C(\omega)) = \mathrm{res}_P(\mu)$. Thus,

$$(8) \qquad c = \mathrm{res}^2_{D,\Delta}(\omega) \in C_\Omega(S, X, D, G).$$

Step 8. Proof of (iii). From now on, assume that X is minimal for the property "X contains $\mathrm{Supp}(c)$". First, notice that, from (4) and (5), we have $D \sim G - K_S - X$. Let us prove that $w(c) \geq X.D$. For that, we prove that X and $\mathrm{Supp}(D)$ have no common irreducible components. Afterwards, we get inequalities satisfied by all the local contributions $m_P(X, D)$ for all $P \in \overline{S}$ and sum them up to get an inequality satisfied by $X.D$.

Sub-step 8.1. First, let us prove that X and $\mathrm{Supp}(D)$ have no common irreducible component. By construction, C is irreducible and not contained in X, thus we just have to check that $\mathrm{Supp}(A)$ and X have no common irreducible component. Assume that $A = A' + X_1$, with $A' \geq 0$ and X_1 is an irreducible component of X. Set $X' := X \setminus X_1$. Then, (4) gives $(\omega) = G - C - X' + A'$. By assumption on the minimality of X, the curve X' avoids at least one point in $\{P_1, \dots, P_s\}$, say P_1 after a suitable reordering of the indexes. Thus, C is the only pole of ω in a neighbourhood of P_1 and, from Proposition 2.1(ii) together with (6), we have $\mathrm{res}^2_{D,P_1}(\omega) = \mathrm{res}^2_{C,P_1}(\omega) = 0$. But, from (8), we have $\mathrm{res}^2_{D,P_1}(\omega) = c_1$ and $c_1 \neq 0$ since by assumption, $P_1 \in \mathrm{Supp}(c)$. This yields a contradiction.

Sub-step 8.2. Now, let us study the intersection multiplicities $m_P(D, X)$ for all $P \in \overline{S}$. First, notice that

$$(9) \qquad \forall P \notin \overline{C}, \ m_P(X, D) \leq 0.$$

Indeed, if $P \notin \overline{C}$, then $m_P(D, X) = m_P(C - A, X) = -m_P(A, X)$ which is negative since A and X are both effective.

To get information on $m_P(X, D)$ for $P \in \overline{C}$, we first study $m_P(C, A - X)$. From [3] Lemma 8.8, we have

$$\forall P \in \overline{C}, \ m_P(C, (\omega) + C) = v_P(\mu),$$

where v_P denotes the valuation at P. From (4), we get

$$\forall P \in \overline{C}, \quad m_P(C, G - X + A) = v_P(\mu)$$
$$m_P(C, A - X) = v_P(\mu) - v_P(G^\star).$$

Afterwards, recall that $(\mu) \geq G^\star - P_1 - \cdots - P_s$ (see Step 3). Moreover, since μ has nonzero residues at the points $P_1, \ldots, P_s$ (its residues at these points are the s first coordinates of c which are assumed to be nonzero), its valuation at these points is equal to -1. Consequently, we obtain

$$(10) \qquad \forall P \in \overline{C}, \ m_P(C, A) - m_P(C, X) \begin{cases} \geq & 0 \quad \text{if } P \notin \{P_1, \ldots, P_s\} \\ = & -1 \quad \text{if } P \in \{P_1, \ldots, P_s\} \end{cases}.$$

Therefore, from Lemma 4.11 together with (10), we get

$$\begin{aligned} \forall P \in \overline{C}, \quad m_P(X, C - A) &\leq m_P(X, C) - \min\{m_P(C, X), m_P(C, A)\} \\ &\leq \begin{cases} 0 & \text{if } P \notin \{P_1, \ldots, P_s\} \\ m_P(C, X - A) & \text{if } P \in \{P_1, \ldots, P_s\} \end{cases}. \end{aligned}$$

Again from (10), if $P \in \{P_1, \ldots, P_s\}$, then $m_P(C, X - A) = 1$. Thus, if we summarise all the information given by the above inequalities together with (9), we get,

$$\forall P \in \overline{S}, \ m_P(X, D) \leq \begin{cases} 0 & \text{if } P \notin \{P_1, \ldots, P_s\} \\ 1 & \text{if } P \in \{P_1, \ldots, P_s\} \end{cases}.$$

Finally, summing up all these inequalities gives

$$X.(G - K_S - X) = X.D \leq s = w(c).$$

$\square$

5. DIFFERENTIAL REALISATION OF THE DUAL OF A FUNCTIONAL CODE

The first possible application of Proposition 4.9 is the following theorem, which answers Question 1b and hence the question raised in the conclusion of [3].

Theorem 5.1. *Let S be a smooth geometrically connected projective surface over $\mathbf{F}_q$, let G be a divisor on S and $P_1, \ldots, P_n$ be rational points of S. Denote by Δ, the 0–cycle $\Delta := P_1 + \cdots, P_n$. Let c be a codeword of $C_L(S, \Delta, G)^\perp$, then there exists a sub–Δ–convenient pair of divisors (D_a, D_b) and a rational 2–form $\omega \in H^0(S, \Omega^2(G - D_a - D_b))$ such that*

$$c := res_{D_a, \Delta}^2(\omega).$$

Moreover, one of the divisors D_a, D_b can be chosen to be very ample.

Before proving Theorem 5.1, let us state a straightforward corollary of it yielding a positive answer for Question 1. That is, even if the dual of a functional code on a smooth surface S is not in general a differential code on S, **it is always a sum of differential codes on this surface**.

Remark 5.2. Actually, using Theorem 5.1, one proves that the dual code $C_L(\Delta, G)^\perp$ is a **union** of differential codes.

Corollary 5.3. *Under the assumptions of Theorem 5.1, there exists a finite family $(D_a^{(1)}, D_b^{(1)}), \ldots, (D_a^{(r)}, D_b^{(r)})$ of sub–Δ–convenient pairs such that*

$$C_L(\Delta, G)^\perp = \sum_{i=1}^{r} C_\Omega(\Delta, D_a^{(i)}, D_b^{(i)}, G).$$

Proof of corollary 5.3. Inclusion $\supseteq$ comes from [3] Theorem 9.1 and Remark 3.1. The reverse inclusion is a consequence of Theorem 5.1 together with the finiteness of the dimension of $C_L(S, \Delta, G)^\perp$. $\square$

Proof of Theorem 5.1. Since S is assumed to be projective, consider some projective embedding of S and let H_S be the corresponding hyperplane section.

From Corollary 4.4, there exists a smooth geometrically irreducible curve X containing all the support of c and such that $X \sim sH_S$ for some positive integer s. Moreover, such a curve X can be chosen with s as large as possible. Therefore, from Lemma 4.5, one can choose X such that $H^1(S, \Omega^2(G-X)) = 0$. Set $D_b := X$ and conclude using Proposition 4.9. □

5.1. **About Theorem 5.1, some comments and an open question.** Unfortunately, the proof of Theorem 5.1 is not constructive. Indeed, this proof involves the existence of a curve X embedded in S such that X is smooth, is linearly equivalent to sH_S for some integer s and such that $H^1(S, \Omega^1(G - X)) = 0$. Poonen's Theorem together with [11] Corollary III.7.8 assert the existence of such a curve provided s is large enough. However, one cannot estimate or find an upper bound for the lowest possible integer s for which such a curve X exists.

Nevertheless, Theorem 5.1 is interesting for theoretical reasons: it extends to surfaces a well-known result for codes on curves. Notice that the construction of a differential code on a surface needs a Δ–convenient pair which is not necessary for the construction of a functional code. Given a functional code $C_L(\Delta, G)$ on a surface S, there is no canonical choice of the (sub–)Δ–convenient pair (D_a, D_b) to construct the code $C_\Omega(\Delta, D_a, D_b, G)$. This lack of canonicity entails the lack of converse inclusion in

$$C_\Omega(\Delta, D_a, D_b, G) \subset C_L(\Delta, G)^\perp.$$

Basically, Theorem 5.1 asserts that $C_L(\Delta, G)^\perp$ can be obtained by summing all the differential codes $C_\Omega(\Delta, D_a^{(i)}, D_b^{(i)}, G)$ for all possible (sub–) Δ–convenient pairs $(D_a^{(i)}, D_b^{(i)})$. Since the dimension of a code is finite, it is sufficient to sum on a finite set of Δ–convenient pairs. This opens the following question.

Question 3. *Under the assumptions of Theorem 5.1, what is the minimal number of differential codes whose sum equals $C_L(S, \Delta, G)^\perp$?*

Example 5.4. This number is 1 when S is the projective plane. Indeed, functional codes on $\mathbf{P}^2$ are Reed–Muller codes (see [13] chapter 13) and it is well-known that the dual of a Reed–Muller code is also Reed–Muller (for instance see [16] XVI.5.8). Thus, the dual of a functional code on $\mathbf{P}^2$ is also functional and, from [3] Theorem 9.6, a functional code can be realised as a differential one.

Example 5.5. It has been proved in [3] Propositions 10.1 and 10.3 that this number is 2 when S is the product of two projective lines.

6. Minimum distance of $C_L(S, \Delta, G)^\perp$

Another application of Proposition 4.9 is to find a lower bound for the minimum distance of a code $C_L(S, \Delta, G)^\perp$. In this section we stay in the classical context yielding codes on a surface which is described in 2.2.1. We also introduce a notation.

Notation 6.1. Denote by $d^\perp$ the minimum distance of $C_L(\Delta, G)^\perp$.

6.1. **The naive approach.** The key of the method is to use Proposition 4.9(iii). Consider a nonzero codeword $c \in C_L(\Delta, G)^{\perp}$. Let X be a curve containing Supp(C), which is minimal for this property and such that $H^1(S, \Omega^2(G-X)) = 0$. Then, Proposition 4.9(iii) asserts that $w(c) \geq X.(G - K_S - X)$.

Basically, one could say that the minimum distance of $C_L(\Delta, G)^{\perp}$ is greater than or equal to the "minimum of $X.(G - K_S - X)$ for all $X \subset S$ satisfying the conditions of Proposition 4.9". Unfortunately, it does not make sense since the set of such integers has no lower bound. Indeed, using Corollary 4.4 together with Lemma 4.5, one sees that for a large enough integer r, there exists a curve $X \sim rH_S$ containing Supp(c), which is minimal for this property (from Corollary 4.4, X can be chosen to be irreducible) and such that $H^1(S, \Omega^2(G - X)) = 0$. Finally, notice that $rH_S.(G - K_S - rH_S) \rightarrow -\infty$ when $r \rightarrow +\infty$.

Thus, the point of the method is to take a minimum in a *good* family of divisor classes, yielding a positive lower bound.

6.2. **The statement.** The main result of the present section involves a set of divisor classes which satisfies some properties. The description of these properties is the point of the following definition.

Definition 6.2. Let δ be a positive integer. A set of divisor classes $\mathcal{D}$ on S is said to satisfy the property $\mathcal{Q}(\Delta, G, \delta)$ if it satisfies the following conditions.

($\mathfrak{V}$) For all $D \in \mathcal{D}$, we have $H^1(S, \Omega^2(G - D)) = 0$.
($\mathfrak{I}$) For all τ–tuple $P_{i_1}, \ldots, P_{i_\tau}$ with $\tau < \delta$, there exists a curve $X \subset S$ whose divisor class is in $\mathcal{D}$ and which contains $P_{i_1}, \ldots, P_{i_\tau}$. Moreover, X is minimal for this property (i.e. any curve $X' \subsetneq X$ avoids at least one point of the τ–tuple $P_{i_1}, \ldots, P_{i_\tau}$).

Notation 6.3. Given a set of divisor classes $\mathcal{D}$ such that the set $\{D.(G - K_S - D), \ D \in \mathcal{D}\}$ has a smallest element, we denote by $\delta(\mathcal{D})$ the integer

$$\delta(\mathcal{D}) := \min_{D \in \mathcal{D}}\{D.(G - K_S - D)\}.$$

Theorem 6.4 (Lower bound for $d^{\perp}$). *In the context described in 2.2.1, let $\mathcal{D}$ be a set of divisor classes on S. If $\mathcal{D}$ satisfies the property $\mathcal{Q}(\Delta, G, \delta(\mathcal{D}))$, then*

$$d^{\perp} \geq \delta(\mathcal{D}) = \min_{D \in \mathcal{D}}\{D.(G - K_S - D)\}.$$

Proof. Let c be a nonzero codeword in $C_L(\Delta, G)^{\perp}$ and assume that $w(c) = \tau < \delta(\mathcal{D})$. Since $\mathcal{D}$ satisfies $\mathcal{Q}(\Delta, G, \delta(\mathcal{D}))$, there exists a curve X containing Supp(c), which is minimal for this property and whose divisor class is in $\mathcal{D}$. Moreover, $H^1(S, \Omega^2(G - X)) = 0$. Therefore, from Proposition 4.9(iii),

$$\tau \geq X.(G - K_S - X) \geq \delta(\mathcal{D}),$$

which yields a contradiction. $\square$

6.2.1. *The arithmetical improvement.* It is possible to improve the bound given by Theorem 6.4 using the maximal number of rational points of an effective divisor whose class is in $\mathcal{D}$. For that, let us introduce a notation.

Notation 6.5. Let D be a divisor class on S. If the corresponding linear system $|D|$ is nonempty, we denote by $\Theta(D)$ the integer

$$\Theta(D) := \max\{\sharp(\text{Supp}(A))(\mathbf{F}_q), \ A \in |D|\}.$$

Theorem 6.6 (Improvement of the lower bound for $d^\perp$). *In the context described in 2.2.1, let $\mathcal{D}$ be a set of divisor classes on S and $\mathcal{E}$ be a subset of $\mathcal{D}$ such that,*

$$\mathcal{E} \supseteq \{D \in \mathcal{D} : \Theta(D) \geq D.(G - K_S - D)\}$$

If $\mathcal{Q}(\Delta, G, \delta(\mathcal{E}))$ is satisfied by $\mathcal{D}$, then

$$d^\perp \geq \delta(\mathcal{E}).$$

Proof. Let c be a nonzero codeword in $C_L(\Delta, G)^\perp$ and assume that $w(c) < \delta(\mathcal{E})$. Since $\mathcal{Q}(\Delta, G, \delta(\mathcal{E}))$ is satisfied by $\mathcal{D}$, there exists a curve X which contains the support of c, is minimal for this property and whose divisor class is in $\mathcal{D}$. Let $D \in \mathcal{D}$ be the divisor class of X. On the one hand, we have,

$$\Theta(D) \geq \sharp X(\mathbf{F}_q) \geq w(c).$$

On the other hand, from Proposition 4.9(iii), we have

$$w(c) \geq D.(G - K_S - D).$$

Thus, $\Theta(D) \geq D.(G - K_S - D)$ and hence $D \in \mathcal{E}$ and $w(c) \geq \delta(\mathcal{E})$. This yields a contradiction. $\square$

6.3. **How to choose $\mathcal{D}$?** The most natural choice for $\mathcal{D}$ is $\mathcal{D} = \{H_S, \dots, aH_S\}$ with a such that $aH(G - K_S - aH) > 0$. From Lemma 4.6, the cohomological vanishing condition of Theorem 6.4 is satisfied by all the elements of $\mathcal{D}$ whenever S is a complete intersection in its ambient space. Afterwards, one checks whether the interpolation condition is satisfied, if it is not (in particular if the condition of minimality is not satisfied), one can try to add some other divisor classes satisfying the cohomological vanishing condition (for instance see 7.2.2).

7. EXAMPLES

In this section we treat some examples of surfaces and obtain lower bounds or exact estimates of the dual minimum distance of a code. The difficult part to apply Theorems 6.4 and Theorem 6.6 is first to choose a good $\mathcal{D}$ and then to compute $\delta(D)$. It becomes easier when the Picard number of the surface (that is the rank of its Neron-Severi group) is small.

Most of the examples we give correspond to surfaces with Picard Number 1. Some examples of surfaces having a larger Picard number are treater and it turns out that surfaces with Picard number 1 yield the better duals of functional codes. Such a remark should be related with the works of Zarzar in [24] who noticed that surfaces with a small Picard number could yield good functional codes.

7.1. **The projective plane.** On $\mathbf{P}^2$, the functional codes are Reed–Muller codes and it is well-known that the dual Reed–Muller code is also a Reed–Muller code ([5] Theorem 2.2.1). The minimum distance of a q–ary Reed–Muller code is well-known (see [5] Theorem 2.6.1). Therefore, the point of the present subsection is not to give any new result but to compare the bound given by Theorem 6.4 to the exact value of the minimum distance in order to check the efficiency of Theorem 6.4.

7.1.1. *Context.* Let H be a line on $\mathbf{P}^2$ and m be a nonnegative integer. Assume that $G := mH$ and $\Delta := P_1 + \cdots + P_{q^2}$ is the sum of all rational points of the affine chart $\mathbf{P}^2 \setminus H$.

7.1.2. *The known results on Reed–Muller codes.* From [5] Theorem 2.2.1, we have $C_L(\Delta, mH)^\perp = C_L(\Delta, (2q - 3 - m)H)$. Moreover, [5] Theorem 2.6.1 asserts that the minimum distance $d^\perp$ of $C_L(\Delta, mH)^\perp$ is

$$(11) \qquad d^\perp = \begin{cases} m + 2 & \text{if} \quad m \leq q - 3 \\ q(m + 3 - q) & \text{if} \quad m \geq q - 2 \end{cases}$$

7.1.3. *Our bounds.* First, recall that $K_{\mathbf{P}^2} \sim -3H$. Therefore,

$$aH.(G - K - aH) = a(m + 3 - a)H^2 = a(m + 3 - a)$$

and this integer is positive for $1 \leq a \leq m + 2$. Then, set $\mathcal{D} := \{H, 2H, \ldots, (m+2)H\}$. This yields $\delta(\mathcal{D}) = m + 2$ (see notation 6.3). Thus, we have to prove that it satisfies the property $\mathcal{Q}(\Delta, G, m+2)$. From Lemma 4.6, this set of divisor classes satisfies the cohomological vanishing condition ($\mathfrak{V}$) (see Definition 6.2). Moreover, for all $l \leq m + 1$ any l–tuple of rational points of $\mathbf{P}^2$ is contained in a curve of degree $\leq m + 2$ and one of them is minimal for this property. Thus, $\mathcal{Q}(\Delta, G, m + 2)$ is satisfied and from Theorem 6.4, we have

$$(12) \qquad \forall m, \ d^\perp \geq m + 2.$$

Now, let us improve the result using Theorem 6.6. First, notice that any configuration of rational points of an affine chart of $\mathbf{P}^2$ is contained in a curve of degree at most q. Therefore, if $m + 2 \geq q$, one can set $\mathcal{D} := \{H, \ldots, qH\}$ and the property $\mathcal{Q}(\Delta, G, s)$ is true for all s. From [19], we have $\Theta(aH) = aq$. Thus, if $m \geq q - 2$, then

$$\Theta(aH) < a(m + 3 - a) \quad \text{for all} \quad a < m + 3 - q.$$

Thus, set $\mathcal{E} := \{(m + 3 - q)H, \ldots, qH\}$. Finally, since $\mathcal{Q}(\Delta, G, s)$ is satisfied by $\mathcal{D}$ for all s, it is in particular satisfied for $s = \delta(\mathcal{E})$. Consequently, from Theorem 6.6, we get

$$(13) \qquad \forall m \geq q - 2, \ d^\perp \geq \delta(\mathcal{E}) = q(m + 3 - q).$$

By comparing (11) with (12) and (13), we see that Theorems 6.4 and 6.6 yield exactly the minimum distance of a Reed–Muller code.

Remark 7.1. By the very same manner one can recover the minimum distance of projective Reed–Muller codes.

7.2. **Quadric surfaces in $\mathbf{P}^3$.** We study the code $C_L(\Delta, G)^\perp$ when S is a smooth quadric in $\mathbf{P}^3$. Recall that there are two isomorphism classes of smooth quadrics in $\mathbf{P}^3$ called respectively *elliptic* and *hyperbolic*. A hyperbolic quadric contains two families of lines defined over $\mathbf{F}_q$ and its Picard group is free of rank 2 and generated by the respective classes E and F of these two families of lines. An elliptic quadric does not contain lines defined over $\mathbf{F}_q$ and its Picard group is free of rank 1 and generated by H_S. We treat separately these two cases (S is hyperbolic and S is elliptic).

7.2.1. *Context.* Let S be a smooth quadric surface in $\mathbf{P}^3$. Let H_S be the scheme-theoretic intersection between S and its tangent plane at some rational point. Let G be $G := mH_S$ for some $m > 0$ and Δ be the sum of all the rational points lying in the affine chart $S \setminus H_S$. The number of these points (and hence the length of the codes) is q^2 and we denote them by $P_1, \ldots, P_{q^2}$.

For all $1 \leq m \leq q - 1$. The dimension of the code $C_L(\Delta, G)$ is equal to

$$(14) \quad \dim C_L(\Delta, G) = \dim \Gamma(S, \mathcal{O}_S(m)) = \binom{m+3}{3} - \binom{m+1}{3} = (m+1)^2.$$

Remark 7.2. For $m \geq q - 1$ we get $C_L(\Delta, G) = \mathbf{F}_q^{q^2}$. Therefore, cases when $m \geq q - 1$ are irrelevant. In what follows, we always assume that $m \leq q - 2$.

Finally, recall that, from [11] Example II.8.20.3,

$$(15) \quad\quad\quad\quad\quad\quad\quad\quad\quad K_S \sim -2H_S.$$

7.2.2. *Hyperbolic quadrics.* If S is a hyperbolic quadric, then, as said before, its Picard group is generated by two lines denoted by E and F. Moreover, $E + F \sim H_S$. As proposed in 6.3, one can set $\mathcal{D} := \{H_S, \ldots, (m+1)H_S\}$. This yields $\delta(\mathcal{D}) = 2m + 2$. Unfortunately, since $m \leq q - 2$, and since S contains rational lines, there are collinear $(m+2)$–tuples of points in $\{P_1, \ldots, P_{q^2}\}$. For such a $(m+2)$–tuple, there exists hypersurface sections of S of degree $\leq m+1$ containing these points but none of them is minimal for this property since such a curve contains the line containing the $(m+2)$–tuple together with another irreducible component.

Therefore, to apply Theorem 6.4, we have to add other divisor classes to $\mathcal{D}$. Therefore, set

$$\mathcal{D} := \{E, F, H_S, \ldots, (m+1)H_S\}.$$

We have $\delta(\mathcal{D}) = m + 2$ and for such a $\mathcal{D}$, the property $\mathcal{Q}(\Delta, G, \delta(\mathcal{D}))$ satisfied. Indeed, since E, F and hypersurface sections of S are complete intersections in $\mathbf{P}^3$, from Lemma 4.6, the cohomological vanishing condition is satisfied. The proof that the interpolating condition ($\mathfrak{I}$) (see Definition 6.2) is also satisfied is left to the reader. Finally, we have the following result.

Proposition 7.3. *The minimum distance $d^\perp$ of $C_L(\Delta, G)^\perp$ satisfies*

$$d^\perp = (\mathcal{D}) = E.((m+2)H_S - E) = m + 2.$$

Proof. The inequality $\geq$ is a consequence of Theorem 6.4. For the converse inequality, consider a rational line L contained in S. After a suitable change of coordinates, one can assume that $P_1, \ldots, P_q \in L$. Therefore, the punctured code $C^\star$ obtained from $C_L(\Delta, G)$ by keeping only the q first coordinates, can be regarded as a code on L, that is a a Reed–Solomon code of length q and dimension $m + 1$. From well–known results on Reed–Solomon codes, its dual has minimum distance $m + 2$ and a minimum weight codeword $c \in C^{\star\perp}$ extended by zero coordinates yields a codeword in $C_L(\Delta, G)^\perp$ with the same weight. $\square$

7.2.3. *Elliptic quadrics.* If S is an elliptic quadric. This time, since it does not contain rational lines, the set

$$\mathcal{D} := \{H_S, \ldots, (m+1)H_S\}$$

satisfies $\mathcal{Q}(\Delta, G, \delta(\mathcal{D}))$. Indeed, from (14), $\dim \Gamma(S, \mathcal{O}_S(m+1)) = (m+2)^2$ which is $> 2m + 1$. Therefore, any $(2m+1)$–tuple of points in $\mathrm{Supp}(\Delta)$ is contained in some curve $C \sim aH_S$ with $a \leq m + 1$. Moreover, since H_S generates the Picard Group of S, for some $a \leq m + 1$ there exists such a curve C which is minimal for this property. This yields the following bound.

Proposition 7.4. *The minimum distance $d^\perp$ of $C_L(\Delta, G)^\perp$ satisfies*

$$d^\perp \geq 2m + 2.$$

Moreover, using Theorem 6.6, it is possible to improve efficiently this bound for some values of m. For that, we have to estimate $\Theta(mH_S)$ for all $m \leq q - 2$ or find an upper bound for it. For that we use what we know about the Picard group of S together with the bound proved by Aubry and Perret in [2] Corollary 3.

Let us give some upper bound for $\Theta(mH_S)$ for some particular values of m.

- $\Theta(H_S) = q + 1$, indeed it is the maximal number of rational points of a plane section of S which is a plane conic.
- $\Theta(2H_S) \leq \max(2(q+1), q+1+\lfloor 2\sqrt{q}\rfloor) = 2q+2$. Indeed, a quadric section of S is either irreducible and has arithmetical genus 1 or reducible. If it is reducible, since the Picard group is generated by H_S, it is the union of two curves both linearly equivalent to H_S and hence the union of to plane sections (i.e. of two plane conics).
- $\Theta(3H_S) \leq \max(3(q + 1), q + 1 + 4\lfloor 2\sqrt{q}\rfloor)$.
- etc...

7.2.4. *Numerical application.* To conclude this section on quadrics, let us compare the parameters $[n, k, d]$ of the code $C_L(\Delta, G)^\perp$ obtained for particular values of q. The following results are obtained using Propositions 7.3, 7.4 and the previous estimates for $\Theta(mH_S)$.

Comparison with Best known codes. In what follows, the minimum distances of the studied codes are compared with the best known minimum distances for given length and dimension appearing in `www.codetables.de` [10] and `http://mint.sbg.ac.at` [18]. These best known minimum distances appear in the right hand column of each array.

For q = 4.

m	Length	Dimension	Minimum Distance		Best Known Distance
			Hyperbolic Quadric	Elliptic Quadric	
1	16	12	3	≥ 4	4
2	16	7	4	≥ 6	8

For q = 8.

m	Length	Dimension	Minimum Distance		Best Known Distance
			Hyperbolic Quadric	Elliptic Quadric	
1	64	60	3	≥ 4	4
2	64	55	4	≥ 6	6
3	64	48	5	≥ 8	11
4	64	39	6	≥ 16 (a)	16
5	64	28	7	24 (b)	24
6	64	15	8	≥ 32 (c)	38

(a) Take $\mathcal{D} := \{H_S, \dots, 4H_S\}$. Since $\Theta(H_S) \leq 9$ and $H_S.(4H_S - K_S - H_S) = 10$, we can choose $\mathcal{E} := \{2H_S, 3H_S, 4H_S\}$. We have $\delta(\mathcal{E}) = 16$ and $\mathcal{Q}(\Delta, G, 16)$ is satisfied by $\mathcal{D}$ since $\dim \Gamma(S, \mathcal{O}_S(4)) = 25 > 16$. Then, apply Theorem 6.6.
(b) Take $\mathcal{D} := \{H_S, \dots, 4H_S\}$. We have $\Theta(2H_S) \leq 18$ and $2H_S.(5H_S - K_S - 2H_S) = 20 > 18$. Take $\mathcal{E} := \{3H_S, 4H_S\}$ and apply Theorem 6.6.
(c) Take $\mathcal{D} := \{H_S, \dots, 5H_S\}$ and $\mathcal{E} := \{4H_S\}$.

Note on the $[64, 28, 24]$ code over $\mathbf{F}_8$. When this article has been submitted, the best $[64, 28]$ code over $\mathbf{F}_8$ on Codetables [10] and MinT [18] had minimum distance 23. However, in [6] Table IIA, Duursma and Chen, assert the existence of a $[64, 28, 24]$ code from the Suzuki curve, without providing further details. After communicating our results to Markus Grassl (from Codetables), he reconstructed our code using *Construction X*, based on two cyclic codes deriving from ours. By this way, he proved by computer that the exact minimum distance is 24. More recently, Iwan Duursma communicated to Markus Grassl a MAGMA script to generate their Suzuki code. He also explained how to deduce the minimum distance of their code. The result comes from a MAGMA computation ([6] §III.B. for $k = 11$) and a duality argument ([14] page 26). Taking these contributions into account, Codetables has been updated.

For $\mathbf{q} = 16$. We do not apply the result for all the possible values of $m \leq q - 2 = 14$ since the array would be too long. Let us only give some of them yielding some relevant codes over the elliptic quadric.

m	Length	Dimension	Minimum Distance		Best Known Distance
			Hyperbolic Quadric	Elliptic Quadric	
8	256	175	10	$\geq$ 32 (a)	46
9	256	156	11	$\geq$ 48 (b)	59
10	256	135	12	$\geq$ 64 (c)	74

(a) Take $\mathcal{D} := \{H_S, \dots, 8H_S\}$. Since $\Theta(H_S) \leq 17$ and $H_S.(8H_S - K_S - H_S) = 18 > 17$, one can take $\mathcal{E} := \{2H_S, \dots, 8H_S\}$.
(b) Take $\mathcal{D} := \{H_S, \dots, 8H_S\}$. Since $\Theta(2H_S) \leq 34$ and $2H_S(9H_S - K_S - 2H_S) = 36 > 34$, one can take $\mathcal{E} := \{3H_S, \dots, 8H_S\}$.
(c) Take $\mathcal{D} := \{H_S, \dots, 8H_S\}$. Since $\Theta(3H_S) \leq 51$ and $3H_S(10H_S - K_S - 3H_S) = 54 > 51$, one can take $\mathcal{E} := \{4H_S, \dots, 8H_S\}$.

7.3. **Cubic surfaces in $\mathbf{P}^3$.** The classification of smooth cubic surfaces is far from being as simple as that of smooth quadrics (see [21]). However, in terms of codes, it is sufficient to separate them into two *sets*, the cubics which contain rational lines and those which do not. As in the case of quadrics, we see that the best codes are given by cubics which do not contain rational lines.

7.3.1. *Context.* The context is almost the same as that of 7.2.1. Let S be smooth cubic surface in $\mathbf{P}^3$, let G be of the form mH_S where H_S is a hyperplane section and Δ be the sum of rational points of S lying out of the support of H_S. For the same reason as in Remark 7.2, we assume that $m \leq q - 2$.

If $m \leq q - 2$, then the dimension of $C_L(\Delta, G)$ equals that of $\Gamma(S, \mathcal{O}_S(m))$ which is

$$(16) \qquad \dim C_L(\Delta, G) = \binom{m+3}{3} - \binom{m}{3} = \frac{3m^2 + 3m + 2}{2}.$$

Remark 7.5. There exists cubic surfaces which does not contain any rational line for instance, explicit examples are given in [24] and [23]. Moreover, it is proved in [12] that such surfaces have Picard number 1.

7.3.2. *Cubics containing rational lines.*

Proposition 7.6. *In the context described in 7.3.1, if S contains rational lines, then the minimum distance $d^\perp$ of $C_L(\Delta, G)^\perp$ satisfies*

$$d^\perp = m + 2.$$

Proof. Let $L_1, \ldots, L_r$ be all the rational lines contained in S. Set $\mathcal{D} := \{L_1, \ldots, L_r, H_S, \ldots, mH_S\}$. A computation gives $\delta(\mathcal{D}) = m + 2$ (the minimum is reached by the lines L_i). By the same manner as Proposition 7.3, the inequality $d^\perp \geq m + 2$ is given by Theorem 6.4 and the equality is obtained using the very same argument as that of Proposition 7.3. $\square$

7.3.3. *Cubics containing no rational lines.* As for elliptic quadrics, we first give a general lower bound based on Theorem 6.4 and then an improvement of it based on Theorem 6.6.

Proposition 7.7. *In the context described in 7.3.1, if S does not contain any rational line, then the minimum distance $d^\perp$ of $C_L(\Delta, G)^\perp$ satisfies*

$$d^\perp \geq 3m.$$

Proof. Set $\mathcal{D} := \{H_S, \ldots, mH_S\}$. We get $\delta(\mathcal{D}) = 3m$. Using (16), one proves easily that $\dim \Gamma(S, \mathcal{O}_S(m)) \geq 3m - 1$ for all m and hence, for all $r < 3m$, any r–tuple of rational points of S is interpolable by some surface section of S of degree $\leq m$ and one of them is minimal for this property. Thus, the result is a consequence of Theorem 6.4. $\square$

It is easy to compare Propositions 7.6 and 7.7 and see that, as in the case of quadrics, cubics containing no rational lines yield much better codes. In what follows, we treat numerical examples based on a cubic with no rational lines and see how to use Proposition 7.7 and how to improve its result in some situations using Theorem 6.6.

7.3.4. *Numerical application.* In [24], the author looked at surfaces with Picard number 1 to get good functional codes $C_L(\Delta, G)$. For that, he noticed that in the classification of cubic surfaces up to isomorphism given by Swinnerton–Dyer in [21] table 1, there exists cubic surfaces which do not contain rational lines and have $q^2 + 2q + 1$ rational points. Some explicit examples of such surfaces are given in [24] and [23]. The following array gives the parameters of codes arising from such a surface over $\mathbf{F}_9$.

m	Length	Dimension	Minimum Distance	Best Known Distance
2	100	90	$\geq\ \ 6$	6
3	100	81	$\geq\ \ 9$	10
4	100	69	$\geq\ \ 12$	16
6	100	36	$\geq\ \ 30\quad(\star)$	40

The box marked with a $(\star)$ corresponds to one where one can apply the improvement given by Theorem 6.6. Indeed, $\Theta(H_S) \leq 9 + 1 + 2\sqrt{9} = 16$.

In the same way, using such an improvement, over $\mathbf{F}_8$, with $m = 5$ one can get a $[81, 35, 24]$–code.

7.4. **Comment and conclusion.** Looking at the results given in [1] and [8] it is clear that codes of the form $C_L(\Delta, H_S)$ and $C_L(\Delta, 2H_S)$ on elliptic quadrics are much better than codes on hyperbolic ones. Such a fact holds probably for codes $C_L(\Delta, G)$ on a quadric for more general divisors G.

The previous result shows that elliptic quadrics yield also better codes of the form $C_L(\Delta, G)^\perp$ that hyperbolic ones. In both cases, the weakness of hyperbolic quadrics comes from the numerous rational lines they contain. This fact can be related to the work of Zarzar who noticed in [24] that one could find good codes of the form $C_L(\Delta, G)$ on surfaces having a small Picard Number. This is well illustrated by quadrics, since hyperbolic quadrics have Picard number 2 and elliptic ones have Picard number 1.

Moreover, the principle asserting that surfaces with a small Picard number yield good codes seems to hold for codes of the form $C_L(\Delta, G)^\perp$. At least, the above examples on quadrics and cubic surfaces encourage to look in this direction. Another explanation makes feel that such surfaces should give good codes: basically, if the Picard number is small, the set of divisor classes $\mathcal{D}$ of Theorem 6.4 may be small and yield a larger candidate $\delta(\mathcal{D})$ for a lower bound of the minimum distance of $C_L(\Delta, G)^\perp$.

Finally, surfaces with small Picard number are twice interesting for coding theory, either for functional codes or for their duals.

Acknowledgements

References

[1] Y. Aubry, *Reed-Muller codes associated to projective algebraic varieties.* Lecture Notes in Math. **1518** (1992), 4–17.

[2] Y. Aubry, M. Perret. *On the characteristic polynomials of the Frobenius endomorphism for projective curves over finite fields.* Finite Fields Appl. **10**(3) (2004), 412–431.

[3] A. Couvreur. *Sums of residues on algebraic surfaces and application to coding theory.* J. of Pure and Appl. Algebra. **213** (2009), 2201–2223.

[4] A. Couvreur. *Résidus de 2-formes différentielles sur les surfaces algébriques et applications aux codes correcteurs d'erreurs*. PhD thesis, Inst. Math. Toulouse (2008). ArXiv:0905.2341.

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

[6] I. Duursma, C.Y. Chen. *Geometric Reed-Solomon codes of length 64 and 65 over $\mathbf{F}_8$*. IEEE Trans. Information Theory. **49**(5) (2003), 1351–1353.

[7] F. A. B. Edoukou. *Codes defined by forms of degree 2 on Hermitian surfaces and Sørensen's conjecture*. Finite Fields Appl. 13(3) (2007), 616–627.

[8] F. A. B. Edoukou. *Codes defined by forms of degree 2 on quadric surfaces*. IEEE Trans. Inform. Theory. **54**(2) (2008), 860–864.

[9] V. D. Goppa. *Codes on algebraic curves*. Dokl. Akad. Nauk SSSR. **259**(6) (1981), 1289–1290.

[10] M. Grassl. *Bounds on the minimum distance of linear codes and quantum codes*. (2007). Accessed on 2010-11-15. `http://www.codetables.de`.

[11] R. Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, 1977.

[12] J. Kollàr, K. E. Smith, A. Corti. *Rational and nearly rational varieties*. Cambridge University Press, 2004.

[13] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*. North-Holland Mathematical Library, 1977.

[14] Martinínez-Moro, Edgar and Munuera, Carlos and Ruano, Diego. *Advances in algebraic codes*. World Scientific, 2008.

[15] A. N. Paršin. *On the arithmetic of two-dimensional schemes. I. Distributions and residues*. Izv. Akad. Nauk SSSR Ser. Mat. **40**(4) (1976), 736–773.

[16] V. S. Pless, W. C. Huffman, R. A. Brualdi. *Handbook of coding theory*. North-Holland Mathematical Library, 1998.

[17] B. Poonen. *Bertini theorems over finite fields*. Ann. of Math. **160**(3) (2004), 1099–1127.

[18] R. Schürer, W. C. Schmid. *MinT: a database for optimal net parameters*. In *Monte Carlo and Quasi-Monte Carlo Methods*. (2006), 457–469. Available online on `http://mint.sbg.ac.at`.

[19] J.-P. Serre. *Lettre à M. Tsfasman*. Astérisque, (**198-200**) (1992), 351–353.

[20] H. Stichtenoth. *Algebraic function fields and codes*. Universitext. Springer-Verlag, 1993.

[21] H. P. F. Swinnerton-Dyer. *The zeta function of a cubic surface over a finite field*. Proc. Cambridge Philos. Soc. **63** (1967), 55–71.

[22] S. G. Vlăduts, Y. I. Manin. *Linear codes and modular curves*. Itogi Nauki i Tekhniki. (1984), 209–257.

[23] F. Voloch, M. Zarzar. *Algebraic geometric codes on surfaces*. SMF Séminaires et congrès, **21** (2009).

[24] M. Zarzar. *Error-correcting codes on low rank surfaces*. Finite Fields Appl., **13**(4) (2007), 727–737.

Alain Couvreur, INRIA Saclay, Projet Tanc, École polytechnique, Laboratoire d'informatique LIX, UMR 7161, 91128 Palaiseau Cedex, France

E-mail address: `alain.couvreur@inria.fr`