HAL open science

The dual minimum distance of arbitrary dimensional algebraic-geometry codes

Alain Couvreur

▶ To cite this version:

Alain Couvreur. The dual minimum distance of arbitrary dimensional algebraic-geometry codes. 2010. inria-00540022v2

HAL Id: inria-00540022

https://inria.hal.science/inria-00540022v2

Preprint submitted on 1 Dec 2010 (v2), last revised 10 Nov 2011 (v3)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

THE DUAL MINIMUM DISTANCE OF ARBITRARY DIMENSIONAL ALGEBRAIC–GEOMETRIC CODES

ALAIN COUVREUR

Abstract. In this article, the minimum distance of the dual $C^{\perp}$ of a functional code C on an arbitrary dimensional variety X over a finite field $\mathbf{F}_q$ is studied. The approach consists in finding minimal configurations of points on X which are not in "*general position*". If X is a curve, the result improves in some situations the well-known *Goppa designed distance*.

AMS Classification: 14J20, 94B27, 14C20.
Keywords: Algebraic geometry, finite fields, error–correcting codes, algebraic–geometric codes, linear systems.

Introduction

A classical problem in coding theory is the estimation of the minimum distance of some code or family of codes constructed on some variety or some family of varieties. For algebraic–geometric codes on curves, one easily gets such a lower bound, frequently called the *Goppa designed distance* (see [13] Definition II.2.4).

On higher–dimensional varieties, the problem becomes really harder even when the geometry of the involved variety is well understood. This difficulty can be explained by a citation from Little in the introduction of a survey on the topic [9]: "the first major difference between higher dimensional varieties and curves is that points on X of dimension ≥ 2 are [...] not divisors". Therefore, if getting the Goppa designed minimum distance is an easy exercice of function fields theory, obtaining any relevant information on the minimum distance of an algebraic–geometric code on a higher–dimensional variety (or a family of varieties) is often the purpose of an entire article. For instance, codes on quadrics are studied in [1], some general bounds on codes on arbitrary–dimensional varieties are given [8] and, in [16], codes on surfaces having a low Neron–Severi rank are studied (the list is far from being exhaustive).

Another kind of codes associated to algebraic varieties can be studied: *the dual of a functional code*. That is, the orthogonal space for the canonical inner product in $\mathbf{F}_q^n$. On a curve X, the dual of a functional code is also a functional code on X (see [13] Proposition II.2.10). It turns out that this result does not hold for higher dimensional varieties. Such a difference with codes on curves has been felt by Voloch and Zarzar who noticed it in [15] and then proved in [2] §10 using an elementary example of surface (or a higher dimensional variety, see [3] Remark II.5.5).

Therefore, on varieties of dimension greater than or equal to 2, one can say that *a new class of codes appears* and it is natural to wonder if this new class contains good codes. This motivates the study of the parameters of these duals of functional codes on arbitrary dimensional varieties, which is the purpose of the present paper.

In the present paper, we will translate the problem of finding the dual minimum distance of an algebraic–geometric code into a problem of finding some particular configuration of points in a projective space. In particular, we will define the elementary

notion of *minimally m–linked points* (Definition 2.8). This notion turns out to be particularly powerful and also nice to deal with. Then, using this notion, one proves Theorem 3.8. This theorem entail Theorem 3.5, which gives estimates or lower bounds for the minimum distance of the duals of functional codes.

The most surprising application of this result is the case when the variety is a plane curve. Ideed, in this situation, since the dual of an algebraic–geometric code on a curve is alo an algebraic–geometric code on this curve, the dual minimum distance has a lower bound given by the Goppa designed distance. Therefore, we will compare the bound yielded by Theorem 3.5 with the Goppa designed distance. It turns out that our bound is better than Goppa's one in two situations. First, when Goppa's bound is negative and hence irrelevant, since our bound is always positive. Second, if one can check some incidence condition on the points of evaluation. In this second situation, one can get a bound which is much better than that of Goppa.

Some proofs of the present paper are long and need the treatment of numerous cases. The study of configurations of points and linear systems having prescribed points in their base locus is often very technical. For instance see the proof of [5] Proposition V.4.3.

Contents. Section 1 is a brief review on algebraic–geometric codes on curves and arbitrary dimensional varieties. Section 2 is devoted to the definition of the notion of *m–general* and *minimally m–linked* configurations of points in a projective space. The connection between this notion and the dual minimum distance is explained in the beginning of Section 3. In addition, Section 3 contains the main theorem (Theorem 3.5) and its "geometric version" (Theorem 3.8). Theorem 3.5 gives lower bounds for the minimum distance of the dual of a functional code. Explicit examples of applications of the main theorem are presented in Section 4. In particular the case of codes on plane curves and the improvements of the Goppa designed distance are studied.

Sections 5 to 9 are devoted to the proof of Theorem 3.8. In Section 5 two key tools for this proof: Lemma 5.1 and Proposition 5.2 are stated. In particular, Lemma 5.1 is the most useful statement of the paper, it is the key of the efficiency of any reasoning based on the notion of minimally m–linked points. Afterwards, sections 6 to 9 are devoted to the proofs of some results on configurations of points in projective spaces, yielding the proof of Theorem 3.5.

1. ALGEBRAIC–GEOMETRIC CODES

Let X be a smooth geometrically connected projective variety defined over a finite field $\mathbf{F}_q$. Let G be a divisor on X and $P_1, \dots, P_n$ be a family of rational points of X avoiding the support of G. Denote by Δ the 0-cycle defined by the formal sum $\Delta := P_1 + \cdots + P_n$. In [14], Manin defines the functional code $C_L(X, \Delta, G)$ to be the image of the map

$$\mathrm{ev}_\Delta : \left\{ \begin{array}{ccc} L(G) & \to & \mathbf{F}_q^n \\ f & \mapsto & (f(P_1), \dots, f(P_n)) \end{array} \right. ,$$

where $L(G)$ denotes the Riemann–Roch space associated to G. When there is no possible confusion on the involved variety, one can remove the "X" and denote this code by $C_L(\Delta, G)$.

As said in the introduction, the aim of this paper is to study the minimum distance of the dual code $C_L(X, \Delta, G)^\perp$.

Caution. A usual abuse of notation in coding theory consists in using the term "dual" to denote the orthogonal space $C^\perp$ of a subspace C of $\mathbf{F}_q^n$ for the canonical inner product.

This space differs from the genuine dual $C^\vee$ of C, which is the space of linear forms on C. According to the conventions in coding theory, we allow ourselves such an abuse of language in this paper, even if actual dual spaces will be also involved sometimes. The exponents $\perp$ and $\vee$ enable to differentiate one "dual" from another, avoiding any confusion.

2. Points in m–general position

2.1. **Context.** In the present section, the base field k is arbitrary.

2.2. **General position in the literature.** The notion of "general position" is classical in algebraic geometry. However, there does not seem to exist any consensual definition. Roughly speaking, a fixed number s of points on a variety X, are said to be in *general position* if they correspond to a point of a Zariski dense subset of the space of configurations of s points of X. The point is that the involved *dense subset* depends on the problem we are working on.

The most usual definition is that s points of the affine space $\mathbf{A}^r_k$ (resp. the projective space $\mathbf{P}^r_k$) are in general position if for all $l \leq r$, no $l+2$ of them lie on a l–dimensional linear subspace. However, several different definitions exist in the literature. For instance, the definition of Hartshorne in [5] V.4 ex 15 differs from that of Mumford in [10] lecture 20.

2.3. **Definition in the present paper.** The definition we will use involves linear independence of evaluation maps on a space of homogeneous forms of fixed degree.

Notation 2.1. We denote by $\mathcal{F}_{m,r}(k)$ the space $\Gamma(\mathbf{P}^r_k, \mathcal{O}_{\mathbf{P}^r_k}(m))$ of homogeneous forms of degree m in $r+1$ variables. If there is no possible confusion on the base field, we denote this space by $\mathcal{F}_{m,r}$.

Notice that the evaluation at a point of X (or a point of $\mathbf{P}^r_k$ actually) does not make sense for homogeneous forms. To avoid this problem, one can choose a system of homogeneous coordinates in $\mathbf{P}^r_k$ and use the evaluation maps defined in [7].

Definition 2.2 ([7] §3)**.** Let $P = (p_0 : \cdots : p_r)$ be a rational point of $\mathbf{P}^r_k$. Let $i \in \{0, \ldots, r\}$ be the smallest integer such that $p_i \neq 0$. For a nonnegative integer m we define the evaluation map to be

$$\mathrm{ev}_P : \left\{ \begin{array}{ccc} \mathcal{F}_{m,r} & \to & k \\ f & \mapsto & \frac{f(p_0,\ldots,p_r)}{p_i^m} \end{array} \right. .$$

Remark 2.3. The previous definition can be regarded as an explicit version of a more conceptual one. Consider a line bundle L on $\mathbf{P}^r_k$ corresponding to $\mathcal{O}_{\mathbf{P}^r_k}(m)$ (such a line bundle is unique up to isomorphism) and choose a system of coordinates on the fiber L_P for each $P \in \mathbf{P}^r(k)$. Then, $\mathrm{ev}_P(f)$ can be defined as the element of k corresponding to $f_P \in L_P$ for this system of coordinates. This is actually the genuine definition used by Manin to define algebraic–geometric codes in [14]. Notice that another choice of coordinates on the fibers L_P gives a Hamming–isometric code.

Now, let us define the notion of m–generality.

Definition 2.4 (m–general position)**.** Let m be a nonnegative integer. A family $P_1, \ldots, P_s$ of rational points of $\mathbf{P}^r$ is said to be in *m–general position* if the evaluation maps $\mathrm{ev}_{P_1}, \ldots, \mathrm{ev}_{P_s}$ are linearly independent in $\mathcal{F}^\vee_{m,r}$.

The following lemma gives a geometric interpretation for the notion of m–generality for $m \geq 1$.

Lemma 2.5. *Let $m \geq 1$ be an integer and $P_1, \ldots, P_s$ be a set of rational points of $\mathbf{P}^r$. Then, the following assertions are equivalent.*

(i) The points $P_1, \ldots, P_s$ are in m–general position.
(ii) The image of the P_i's after the mth Veronese embedding are in 1–general position (or in "general position" for the "usual" definition sketched in the beginning of the present section).
(iii) For all $i \in \{1, \ldots, s\}$, there exists a hypersurface H_i of degree m in $\mathbf{P}^r$ containing the P_j's for all $j \neq i$ and avoiding P_i.
(iv) For all $i \in \{1, \ldots, s\}$, the point P_i is not a base point of the linear system of hypersurfaces of degree m in $\mathbf{P}^r$ containing all the P_j's for $j \neq i$.
(v) The linear system Γ of hypersurfaces of degree m in $\mathbf{P}^r$ containing the points $P_1, \ldots, P_s$ has dimension

$$\dim \Gamma = \dim \mathcal{F}_{m,r} - 1 - s.$$

Proof. It is an elementary exercise of linear algebra. □

Remark 2.6. Notice that Definition 2.4 makes sense even if $m = 0$. However, this case is removed in Lemma 2.5 since items (iii), (iv) and (v) do not make sense for $m = 0$.

Remark 2.7. The notion of 1–generality corresponds to the "usual" definition of general position, which is described in the beginning of the present section. In $\mathbf{P}^r$, a s–uplet of points is in 1–general position if the points are projectively independent, or equivalently if and only if they generate a $(s-1)$–dimensional linear subspace of $\mathbf{P}^r$.

Definition 2.8. A family $P_1, \ldots, P_s$ of rational points of $\mathbf{P}^r$ is said to be *m–linked* if they are not in m–general position. It is said to be *minimally m–linked* if it is m–linked and if each proper subset of $\{P_1, \ldots, P_s\}$ is in m–general position.

We will see further that the notion of being *minimally m–linked* is very useful for error–correcting codes. Lemma 2.12 gives some elementary algebraic and geometric translations of this definition which will be very often used in what follows.

Lemma 2.9. *Let $m \geq 1$ be an integer. A family $P_1, \ldots, P_s$ of rational points of $\mathbf{P}^r$ is minimally m–linked if and only if there exists at least one non-trivial relation of the form $\lambda_1 ev_{P_1} + \cdots + \lambda_s ev_{P_s} = 0$ and that, for all such relation, the λ_i's are all nonzero.*

Proof. It is an elementary exercise of linear algebra. □

Remark 2.10. For dimensional reasons, one can prove easily that the number of elements of an m–general family of points in $\mathbf{P}^r$ is at most $\dim \mathcal{F}_{m,r}$ and that of a minimally m–linked family is at most $\dim \mathcal{F}_{m,r} + 1$.

Remark 2.11. Let $P_1, \ldots, P_s$ be a family of points in $\mathbf{P}^r$ and let m be a nonnegative integer. Assume that $s \leq \dim \mathcal{F}_{m,r}$, then the P_i's are minimally m–linked if and only if for all $i_0 \in \{1, \ldots, s\}$ the linear system of hypersurfaces of degree m containing the points $P_1, \ldots, P_{i_0-1}, P_{i_0+1}, \ldots, P_s$ is nonempty and has P_{i_0} as a base point.

Remark 2.12. The previous remark entails that, to prove that a family of points $P_1, \ldots, P_s \in \mathbf{P}^r$ with $s \leq \dim \mathcal{F}_{m,r}$ is *not* minimally m–linked, it is sufficient to prove that for one of these points P_{i_0}, there exists a hypersurface of degree m containing the P_j's for $j \neq i_0$ and avoiding P_{i_0}.

We conclude the present section with Lemma 2.13, which is crucial in the present paper. Indeed, it enables to work over an algebraically closed field of the form $\overline{\mathbf{F}}_q$ in order to get information on the minimum distance of some codes, even if a code is a vector space of a finite field $\mathbf{F}_q$. Such a "geometrisation" of the problem is very useful since over infinite fields, the positive dimensional linear systems have infinitely many elements.

Lemma 2.13. *Let $P_1, \dots, P_s$ be a family of rational points of $\mathbf{P}^r_k$. Let L be an algebraic extension of k. Then, the points $P_1, \dots, P_s$ are in m–general position (resp. are m–linked, resp. are minimally m–linked) in $\mathbf{P}^r_k$ if and only if they are in m–general position (resp. are m–linked, resp. are minimally m–linked) in $\mathbf{P}^r_L$.*

Proof. Linearly independent (resp. linked) vectors in $\mathcal{F}_{m,r}(k)^\vee$ remain independent (resp. linked) in $\mathcal{F}_{m,r}(L)^\vee = \mathcal{F}_{m,r}(k)^\vee \otimes_k L$. □

3. Duals of algebraic–geometric codes

In what follows, when we deal with algebraic–geometric codes and only in this situation (that is in the present section and in Section 4), we will always stay in the following context.

3.1. **Context and notations.** In what follows, X is a smooth geometrically connected projective variety over $\mathbf{F}_q$, which is a **complete intersection** in some projective space $\mathbf{P}^r$ for some $r \geq 2$. Moreover, m is a nonnegative integer and G_m is a divisor on X which is linearly equivalent to a scheme–theoretic intersection of X with a hypersurface of degree m. In addition, $P_1, \dots, P_n$ is a family of rational points of X avoiding the support of G_m and we denote by Δ the 0–cycle $\Delta := P_1 + \cdots + P_n$.

From [5] II.8 exercise 4, the variety X is *projectively normal* (see [5] I.3 exercise 18 for a definition) and an element of $L(G_m)$ can be identified to a restriction to X of an element of $\mathcal{F}_{m,r}$. The connection between minimum distance of $C_L(\Delta, G_m)^\perp$ and the notion of m–generality lies in the elementary Lemma 3.3 below.

3.2. **Codewords of the dual and configurations of points.** First, let us notice a usual abuse of language, in the next sections.

Abuse of language. In what follows, given a codeword $c \in C_L(\Delta, G_m)$ or $c \in C_L(\Delta, G_m)^\perp$, we will call *support of* c the set of points $P_{i_1}, \dots, P_{i_s}$ in $\mathrm{Supp}(\Delta)$ corresponding to the nonzero coordinates of c.

Thanks to the following proposition, the problem of finding a lower bound for the minimum distance of the code $C_L(\Delta G)^\perp$ is translated into that of finding configurations of (minimally) m–linked in the points of the support of Δ.

Proposition 3.1. *The minimum distance of the code $C_L(\Delta, G_m)^\perp$ is the smallest number of m–linked points in the support of Δ.*

Remark 3.2. Equivalently it is the smallest number of *minimally* m–linked points of $\mathrm{Supp}(\Delta)$.

The proof of Proposition 3.1 is a straightforward consequence of the following lemma.

Lemma 3.3. *There exists a nonzero codeword $c \in C_L(\Delta, G_m)^\perp$ with support contained in $\{P_{i_1}, \dots, P_{i_s}\}$ if and only if these points are m–linked. Furthermore, if these points are minimally m–linked, then the support of such a codeword is equal to $\{P_{i_1}, \dots, P_{i_s}\}$.*

Proof. The existence of the codeword $c \in C_L(\Delta, G_m)^\perp$ with support $\{P_{i_1}, \dots, P_{i_s}\}$ entails that of a nonzero linear relation linking the evaluation maps $\mathrm{ev}_{P_{i_1}}, \dots, \mathrm{ev}_{P_{i_s}}$ in $\mathcal{F}^\vee_{m,r}$. Conversely, if $P_{i_1}, \dots, P_{i_s}$ are m-linked, then a non-trivial linear relation linking the corresponding evaluation maps entails the existence of a nonzero codeword with support contained in $\{P_{i_1}, \dots, P_{i_s}\}$. If the points are minimally m–linked, then, from Lemma 2.9, a non-trivial linear relation linking the corresponding evaluation maps gives a codeword with support equal to $\{P_{i_1}, \dots, P_{i_s}\}$. □

Therefore, minimally m–linked or configurations of points seem to be useful in order to estimate the minimum distance of $C_L(\Delta, G_m)^\perp$. Let us state the main results concerning the minimum distance of the dual of a functional code.

3.3. **Lower bounds for the minimum distance of the dual code.** To state some results on the minimum distance of the codes of the form $C_L(\Delta, G_m)^\perp$, we will treat separately the "small" values of m, i.e. $m = 0$ and 1 and the other ones, i.e. $m \geq 2$.

3.3.1. *Small values of m.* If $m = 0$, then the code $C_L(\Delta, G_0)$ is a *pure repetition code*, i.e. it is generated over $\mathbf{F}_q$ by the codeword $(1, \dots, 1)$. Thus, the minimum distance of $C_L(\Delta, G_0)^\perp$ is 2 and any pair of distinct points $P_i, P_j \in \mathrm{Supp}(\Delta)$ is the support of a codeword in $C_L(\Delta, G_0)^\perp$. In terms of m-generality one sees easily that one point is always 0–general and that two distinct points are always 0–linked and hence minimally 0–linked.

If $m = 1$, then we have the following result.

Lemma 3.4. *In the context described in 3.1, if for all $t \leq n-2$, no $t+2$ of the P_i's lie on a linear subspace of dimension t, then the minimum distance of $C_L(\Delta, G_1)^\perp$ is n. Moreover, let s be the smallest integer such that there exists $s+2$ elements of Supp(Δ) lying in a linear subspace of dimension s. Then $s+2$ is the minimum distance of the code $C_L(\Delta, G_1)^\perp$.*

Proof. From Remark 2.7, a t–uplet of points of $\mathbf{P}^r$ is 1–general if and only if it generates a linear subspace of dimension $t-1$. If the integer s of the statement exists, then the smallest number of 1–linked points of Supp(Δ) is $s+2$ and, from Proposition 3.1, this gives the minimum distance of $C_L(\Delta, G_1)^\perp$. If s does not exist, then the minimum distance of $C_L(\Delta, G_1)^\perp$ is obviously n. □

3.3.2. *Other values of m.*

Theorem 3.5. *In the context described in 3.1, let m be an integer greater than or equal to 2 and d be the minimum distance of the code $C_L(\Delta, G_m)^\perp$. Then,*

(i) $d = m+2$ if and only if $m+2$ of the P_i's are collinear in $\mathbf{P}^r$;
(ii) $d = 2m+2$ if and only if no $m+2$ of the P_i's are collinear and $2m+2$ of them lie on a plane conic (possibly reducible);
(iii) $d = 3m$ if and only if no $m+2$ of the P_i's are collinear, no $2m+2$ of them lie on a plane conic and $3m$ of them are coplanar and lie at the intersection of a cubic and a curve of degree m having no common irreducible component;
(iv) $d \geq 3m+1$ if and only if no sub-family of the P_i's satisfies one of the three above-cited configurations.

Moreover, in case (i) (resp. (ii), resp. iii), the supports of the minimum weight codewords are the $(m+2)$–uplets of collinear points (resp. the $(2m+2)$–uplets of points lying on a plane conic, resp. the $(3m)$–uplets of points lying at the intersection of two coplanar curves with respective degrees 3 and m) in $\{P_1, \dots, P_n\}$.

c

Remark 3.6. If $m = 2$, then the condition of Theorem 3.5(iii) cannot happen. Consequently, in this situation, the statement is simplified: *the minimum distance d of $C_L(\Delta, G_2)^\perp$ is*

(i) 4 *if and only if* 4 *of the P_i's are collinear;*
(ii) 6 *if and only if* 6 *of the P_i's lie on a plane conic;*
(iii) ≥ 7 *if and only if none of the above-cited configurations happens.*

Therefore, in Section 9, which is devoted to the end of the proof of Theorem 3.5, we will assume that $m \geq 3$.

Remark 3.7. If $m \geq 2$, one checks that $m + 2$, $2m + 2$ and $3m$ are lower than or equal to $\dim \mathcal{F}_{m,r}$ (recall that we are in the context 3.1 and hence $r \geq 2$). Therefore, to prove that $m + 2$, $2m + 2$ or $3m$ points are (resp. are not) minimally m–linked, one can use Remark 2.11 (resp. Remark 2.12).

To prove Theorem 3.5, we will actually prove the following statement, which is a "geometric version" of Theorem 3.5.

Theorem 3.8 (Geometric version of Theorem 3.5)**.** *Let $P_1, \ldots, P_n$ be a family of distinct points in a projective space $\mathbf{P}^N$ and let $m \geq 2$ be an integer. Then, the smallest number of m–linked points in $\{P_1, \ldots, P_n\}$ is*

(i) $m + 2$ *iff* $m + 2$ *of the P_i's are collinear;*
(ii) $2m + 2$ *iff no* $m + 2$ *of the P_i's are collinear and* $2m + 2$ *of the P_i's lie on a plane conic;*
(iii) $3m$ *iff no* $m+2$ *of the P_i's are collinear and no* $2m+2$ *of them lie on a plane conic and* $3m$ *of them lie at the intersection of two coplanar plane curves of respective degrees* 3 *and* m*;*
(iv) $> 3m$ *iff the P_i's do not satisfy any of the above configurations.*

The proof of Theorem 3.8 will be the purpose of Sections 6 to 9. The organisation of this proof is detailed in 3.4 below.

First let us show that Theorem 3.8 entails Theorem 3.5.

Proof of Theorem 3.8 $\Rightarrow$ Theorem 3.5. Proposition 3.1 asserts that the minimum distance of $C_L(\Delta, G_m)^\perp$ equals the smallest number of the P_i's which are m–linked (and hence minimally m–linked). Therefore, Theorem 3.8(X) $\Rightarrow$ Theorem 3.5(X) for all X in {i, ii, iii, iv}. □

3.4. **The proof of Theorem 3.8.** In Section 5, Lemma 5.1 and Proposition 5.2 are proved. These statements are key tools for the proof of Theorem 3.8. Lemma 5.1 is a powerful way to handle the notion of being *minimally m–linked*. Proposition 5.2 gives plenty of configurations of m–linked points. Among others things, it entails that $m + 2$ collinear points, $2m + 2$ points on a plane conic or $3m$ points lying at the intersection of two coplanar curves with respective degrees m and 3 are m–linked.

In Section 6, one proves Proposition 6.1 asserting that less than $m+1$ points of $\mathbf{P}^r$ are always in m–general position. Proposition 6.1 together with Proposition 5.2 (applied to $a = 1$) entail obviously the *"if"* part of Theorem 3.8(i). Afterwards, we prove Proposition 6.2 which asserts that, conversely, any m–linked configuration of $m + 2$ points is always a family of collinear points. This yields the *"only if"* part of Theorem 3.8(i).

In Section 7, we prove Proposition 7.2, which asserts that any set of at most $2m+1$ points of $\mathbf{P}^r$ such that no $m+2$ of them are collinear is in m–general position. Proposition 7.2 in addition with Proposition 5.2 (applied to $a=2$), entail the *"if"* part of Theorem 3.8(ii). Afterwards, one proves Proposition 7.4, which asserts that, conversely, any m–linked configuration of $2m+2$ points such that no $m+2$ of them are collinear lie on a plane conic. This yields the *"only if"* part of Theorem 3.8(ii).

In Section 8, we prove Proposition 8.1, which asserts that any set of at most $3m-1$ points of $\mathbf{P}^r$ such that no $m+2$ of them are collinear and no $2m+2$ of them lie on a plane conic, are in m–general position. Proposition 8.1 in addition with Proposition 5.2 (applied to $a=3$) yields the *"if"* part of Theorem 3.8(iii).

Section 9 is devoted to the proof of Proposition 9.1, which asserts that any m–linked configuration of $3m$ points such that no $m+2$ of them are collinear and no $2m+2$ of them are on a plane conic is a set of coplanar points lying at the intersection of a cubic and a curve of degree m having no common component. This concludes the proof of Theorem 3.8 since the *"only if"* part of (iii) and (iv) are straightforward consequences of Proposition 9.1.

Before starting the different steps of the proof of Theorem 3.5, let us present some applications of it.

4. Examples and applications

Even if the objective of the present article is to get some information on duals of algebraic–geometric codes on higher dimensional varieties, Theorem 3.5 holds for varieties of any dimension. Surprisingly, when the variety X is a plane curve, Theorem 3.5 gives a relevant lower bound for the minimum distance of some algebraic–geometric codes on X, when the Goppa designed distance is negative and hence irrelevant.

4.1. **Algebraic–geometric codes on plane curves.**

4.1.1. *Context.* Let a be a positive integer. Let $X \subset \mathbf{P}^2$ be a smooth projective plane curve of degree a over $\mathbf{F}_q$. Let m be a nonnegative integer, L be a line of $\mathbf{P}^2$ and G_m be the pullback of mL by the natural inclusion map $X \hookrightarrow \mathbf{P}^2$. Let $P_1, \ldots, P_n$ be n rational points of X avoiding the support of G_m and denote by D the divisor $D := P_1 + \cdots + P_n$.

4.1.2. *The code $C_L(D, G_m)^\perp$.* From [13] Theorem II.2.8, the dual $C_L(D, G_m)^\perp$ of the functional code is the *differential* code denoted by $C_\Omega(D, G_m)$. Denote by d the minimum distance of $C_L(D, G_m)^\perp$. Let δ_G be the *Goppa designed distance.* From, [13] Theorem II.2.7, we have $\delta_G = \deg(G_m) - (2g_X - 2)$, where g_X denotes the genus of X, which is $g_X = (a-1)(a-2)/2$. This gives

$$(\Delta G) \qquad \delta_G = a(m+3-a).$$

We know that $d \geq \delta_G$. Let us study the lower bound for d given by Theorem 3.5.

4.1.3. *Lower bound for the dual minimum distance.* First, notice that if the degree of the curve X is 1 or 2, then X is isomorphic to $\mathbf{P}^1$ and the codes on it are Reed–Solomon codes, for which the Goppa designed distance equals the genuine distance (which reaches the Singleton bound) and hence is optimal. Therefore, from now on, assume that the degree a of X is greater than or equal to 3.

Denote by δ the lower bound for the minimum distance given by Theorem 3.5:

$$\delta = \begin{cases} m+2 & \text{if } 0 \leq m \leq a-2 \\ 2m+2 & \text{if } m = a-1 \\ 3m & \text{if } m \geq a \end{cases}.$$

Notice that δ is always positive, which is not true for the Goppa designed distance δ_G. Therefore δ gives a relevant lower bound for the minimum distance of $C_L(D, G_m)^\perp$ when $\delta_G \leq 0$.

Theorem 4.1 (Minimum distance for codes on curves)**.** *Let X be a smooth plane curve of degree $a \geq 3$ and consider the code $C_\Omega(D, G_m) = C_L(D, G_m)^\perp$. Then, $\delta > \delta_G$ if and only if $\delta_G \leq 0$ (or equivalently, if and only if $m \leq a-3$). In other words, δ improves the Goppa designed distance δ_G as a lower bound for the minimum distance of the code whenever δ_G is negative and hence irrelevant for coding theory.*

Proof. Let us compare the numbers δ and δ_G. Using (ΔG), a brief computation gives

$$\delta - \delta_G = \begin{cases} (a-1)(a-2-m) & \text{if } 0 \leq m \leq a-2 \\ 0 & \text{if } m = a-1 \\ (a-3)(a-m) & \text{if } m \geq a \end{cases}.$$

Consequently, $\delta - \delta_G > 0$ if and only if $m \leq a-2$. That is, from (ΔG), this difference is nonnegative if and only if the Goppa designed distance δ_G is negative. □

Remark 4.2. In the proof, one can also see that $\delta = \delta_G$ for all $m \in \{a-3, a\}$.

Example 4.3. Consider the finite field $\mathbf{F}_{64}$ and the curve C of equation

$$F_C := w^{24}x^{11} + w^{44}x^6y^2z^3 + w^{24}x^5yz^5 + w^{20}x^4y^6z + w^{33}x^2z^9 +$$
$$w^{46}xy^5z^5 + w^{46}xz^{10} + w^{39}y^{11} + w^{30}y^2z^9,$$

where w is a primitive element of $\mathbf{F}_{64}$ over $\mathbf{F}_2$ with minimal polynomial $x^6 + x^4 + x^3 + x + 1$. This curve has 80 rational points in the affine chart $\{z \neq 0\}$ and 1 rational point *at infinity*. Using the previous results, one sees that the Goppa designed distance of $C_L(D, G_m)^\perp$ is negative for $m \geq 8$. Using Theorem 3.5, we prove that the code $C_L(D, G_m)^\perp$ for $m = 1 \ldots 8$ are respectively of the form: $[80, 77, \geq 3]$, $[80, 74, \geq 4]$, $[80, 70, \geq 5]$, $[80, 65, \geq 6]$, $[80, 59, \geq 7]$, $[80, 52, \geq 8]$, $[80, 46, \geq 9]$ and $[80, 35, \geq 10]$.

Afterwards, under some geometric condition on the points $P_1, \ldots, P_n$, one can improve the Goppa designed distance by using Theorem 3.5. It is worth to notice that if the lower bound $m+2$ is not reached (that is, if no $m+2$ of the P_i's are collinear), then this bound jumps directly to $2m+2$. By this way one can get, under some non incidence conditions, some good improvements of the Goppa bound even if it is positive.

Theorem 4.4. *Under the assumptions of Theorem 4.1,*

(1) if $m \leq a-2$ and no $m+2$ of the P_i's are collinear, then the minimum distance d of $C_L(D, G_m)^\perp$ satisfies $d \geq 2m+2$ and this bound improves that of Goppa;
(2) if $m \leq a-1$, no $m+2$ of the P_i's are collinear and no $2m+2$ of them lie on a conic, then $d \geq 3m$ and this bound improves that of Goppa;
(3) if $m \leq a$, the P_i's do not satisfy any of the above condition and no $3m$ of them lie on a cubic, then $d \geq 3m+1$ and this bound improves that of Goppa.

Proof. It is a straightforward consequence of Theorem 3.5. □

Example 4.5. Back to example 4.3, a computation using the Software MAGMA yields only one line containing at least 7 of the P_i's. It is the line L of equation $x = 0$, which contains 10 of the P_i's. Therefore by removing 4 (resp. 3, resp. 2, resp 1) of the P_i's on L, one gets a divisor $D^{(4)}$ (resp. $D^{(3)}$, resp. $D^{(2)}$, resp. $D^{(1)}$) and the codes $C_L(D^{(i)}, G_5)^\perp$ for $i \in \{1, 2, 3, 4\}$ are respectively of the form $[76, 55, \geq 12]$, $[77, 49, \geq 14]$, $[78, 44, \geq 16]$ and $[79, 34, \geq 18]$.

Moreover, the Goppa designed distance asserts that $C_L(D, G_9)^\perp$ has a minimum distance greater than or equal to 11. However, since no 11 of the P_i's are collinear, Theorem 4.4 asserts that this minimum distance is greater than or equal to 20. Thus, **the obtained lower bound is** 9 **units bigger than that of Goppa**.

The previous example presents actually a good method to get good codes on curves by selecting the points of evaluation . Indeed, assume there are only few lines (resp. conics, resp. cubics) containing $m + 2$ (resp. $2m + 2$, resp. $3m$) of the P_i's. Then one can remove some points of these lines (resp. conics, resp. cubics) such that the lower bound for the minimum distance jumps to $2m + 2$ (resp. $3m$, resp $3m + 1$).

Further, in 5.4, we will give an interpretation of the Goppa designed distance for plane curves in terms of minimally m-linked points in $\mathbf{P}^2$.

4.2. **Surfaces in $\mathbf{P}^3$.** In 4.2, we assume that $q \geq 3$. The binary case will be trated in 4.4.

4.2.1. *Context.* Let a be a positive integer and X be a smooth projective geometrically connected surface of degree a defined over $\mathbf{F}_q$ and embedded in $\mathbf{P}^3$. Let H be a plane of $\mathbf{P}^3$, let m be a nonnegative integer and G_m be the pullback of the divisor mH by the canonical inclusion $X \hookrightarrow \mathbf{P}^3$. Let $P_1, \ldots, P_n$ be a family of rational points of X avoiding the support of G_m and Δ be the 0–cycle $\Delta := P_1 + \cdots + P_n$.

4.2.2. *Duals of codes on quadrics.* Let X be a quadric in $\mathbf{P}^3$. There are two isomorphism classes of smooth quadrics in $\mathbf{P}^3$, respectively called *hyperbolic* and *elliptic* quadrics. Hyperbolic quadrics contain lines defined over $\mathbf{F}_q$ and elliptic quadrics do not.

For each isomorphism class, there exists an affine chart U of X containing exactly q^2 rational points. One choses the complement of U to be the support of G_m and the sum of the rational points of U to be Δ.

Theorem 4.6. *The minimum distance d of $C_L(\Delta, G_m)^\perp$ satifies the following relations.*

$$\textit{If } X \textit{ is hyperbolic, then } \begin{cases} d = m + 2 & \textit{if} \quad m \leq q - 2 \\ d = 2m + 2 & \textit{if} \quad m = q - 1 \\ d = 3m & \textit{if} \quad m = q \\ d > 3m & \textit{if} \quad m > q \end{cases}.$$

$$\textit{If } X \textit{ is elliptic, then } \begin{cases} d = 2m + 2 & \textit{if} \quad m \leq (q-1)/2 \\ d > 3m & \textit{if} \quad m > (q-1)/2 \end{cases}.$$

Proof. Notice that, since the P_i's all lie on an affine chart of $\mathbf{P}^3$, no $q + 1$ of them are collinear and no $2q + 1$ of them lie on a conic. If X is hyperbolic (resp. elliptic), then plane sections of X are either irreducible plane conic containing at most $q + 1$ of the P_i's, or a union of two rational lines (resp. a union of two lines defined over $\mathbf{F}_{q^2}$ and conjugated by the Frobenius) containing at most $2q$ of the P_i's (resp. containing 1 of the P_i's). This description of the plane sections of X and Theorem 3.5 lead easily to the expected result. □

Example 4.7. For $q = 3$ one gets codes of the following form.

	X is hyperbolic	X is elliptic
$m = 1$	$[9, 5, 3]$	$[9, 5, 4]$

For $q = 4$ one gets codes of the following form.

	X is hyperbolic	X is elliptic
$m = 1$	$[16, 12, 3]$	$[16, 12, 4]$
$m = 2$	$[16, 7, 4]$	$[16, 7, \geq 7]$

For $q = 5$ one gets codes of the following form.

	X is hyperbolic	X is elliptic
$m = 1$	$[25, 21, 3]$	$[25, 25, 4]$
$m = 2$	$[25, 16, 4]$	$[25, 16, 6]$
$m = 3$	$[25, 9, 5]$	$[25, 9, \geq 9]$

4.2.3. *Duals of codes on cubics.* Let X be a cubic in $\mathbf{P}^3$. As in the previous case we will state a result about the dual minimum distance of a functional code on X, by separating the cases when X contains rational lines and when it does not. Indeed, even if a cubic surface always contains 27 lines over the algebraic closure of the base field, all of these lines can be non rational (for instance, see [6] chapter 3).

Theorem 4.8. *The minimum distance d of $C_L(\Delta, G_m)^\perp$ satisfies the following relations.*

If X contains rational lines, then $\begin{cases} d = m + 2 & \text{if } m \leq q - 2 \\ d = 2m + 2 & \text{if } m = q - 1 \\ d \geq 3m & \text{if } m \geq q \end{cases}$.

If X does not contain any rational line, then $\begin{cases} d \geq 3 & \text{if } m = 1 \\ d \geq 6 & \text{if } m = 2 \\ d \geq 3m & \text{if } m \geq q \end{cases}$.

Proof. As in the previous example, since the P_i's lie on an affine chart of $\mathbf{P}^3$, no $q+1$ of them are collinear and no $2q+1$ of them lie on a conic. Moreover, if the cubic surface X does not contain rational lines, then it does not contain any rational plane conic. This yields the result thanks to Theorem 3.5. □

Example 4.9. The Hermitian surface over $\mathbf{F}_4$ is the surface of equation $x^3+y^3+z^3+t^3 = 0$. This surface has 36 rational points in the affine chart $\{t \neq 0\}$ and contains plenty of lines. The code $C_L(\Delta, G_1)^\perp$ is $[36, 32, 3]$ and the supports of the codewords of weight 3 are triples of collinear points. The code $C_L(\Delta, G_2)^\perp$ is $[36, 26, 4]$ and the supports of the codewords of weight 3 are 4–uplets of collinear points. The code $C_L(\Delta, G_3)^\perp$ is $[36, 17, 8]$ and the supports of the codewords of weight 3 are 8–uplets of points lying on plane conics (since $q = 4$, such conics are reducible).

Example 4.10. In [16], an example of a cubic surface over $\mathbf{F}_9$ containing no rational lines is given. The author proves that on this surface, the code $C_L(\Delta, G_2)$ is a $[100, 10, 68]$ code. Using Theorem 4.8, one proves that its dual is a $[100, 90, \geq 6]$ code. Theorem 4.8 asserts also that $C_L(\Delta, G_3)^\perp$ is $[100, 81, \geq 9]$.

Example 4.11. Another example is given in [15]: the surface over $\mathbf{F}_3$ defined by the affine equation $x^3 + y^3 + z^3 - zx^2 - yx^2 - yz^2 + xz^2 + 1$. The code $C_L(\Delta, G_1)$ on this surface is $[13, 4, 7]$. From Theorem 4.8, it dual is a $[13, 9, \geq 3]$ code.

Moreover, the authors also assert that this surface does not contain any rational line over $\mathbf{F}_9$. They prove that, over $\mathbf{F}_9$, the code $C_L(\Delta, G_2)$ is $[91, 10, 61]$. Theorem 4.8

entails that its dual is $[91, 81, \geq 6]$. Moreover, Theorem 4.8 entails that $C_L(\Delta, G_3)^\perp$ is a $[91, 72, \geq 9]$ code over $\mathbf{F}_9$.

4.2.4. *Surfaces of higher degree.* To conclude this subsection on codes on surfaces, let us give some example of surfaces of higher degree. Notice that, Theorem A.1 together with Remark A.2 assert that almost all surfaces in $\mathbf{P}^3$ of degree ≥ 4 do not contain any line, plane conic and plane cubic, even over the algebraic closure of their based field. Moreover, we produced a MAGMA program checking all the plane sections of a surface and asserting whether they are all irreducible.

Thus, one can expect to find a lot of surfaces giving dual codes of minimum distance $> 3m$.

Example 4.12. Over $\mathbf{F}_7$, the surface defined by the equation $x^4 + 2x^3y + 4x^3t + 3x^2z^2 + 6xy^3 + 4xz^2t + 4y^3z + 6y^2t^2 + 5yt^3 + 4z^4$ does not contain any line, plane conic or plane cubic. It has 54 rational points in the affine chart $\{t \neq 0\}$. Therefore, Theorem 3.5 asserts that the codes $C_L(\Delta, G_m)^\perp$ are respectively of the form $[54, 50, \geq 3]$, $[54, 44, \geq 4]$, $[54, 34, \geq 9]$ and $[54, 20, \geq 12]$ when $m = 1, 2, 3, 4$.

Example 4.13. Over $\mathbf{F}_8$, the surface defined by the affine equation $\gamma^2x^5 + x^4y + \gamma^5x^4z + \gamma^4x^3zt + \gamma^6x^2z^3 + \gamma^4xyt^3 + \gamma^3xz^4 + \gamma^5y^4t + \gamma^3y^2t^3 + \gamma^6yz^4 + \gamma^5yt^4 + \gamma^5z^2t^3$, where γ denotes a primitive element of $\mathbf{F}_8/\mathbf{F}_2$, contains also no line, plane conic or plane cubic. Its affine chart $\{t \neq 0\}$ contains 64 rational points and hence, the codes $C_L(\Delta, G_m)^\perp$ are of the form $[64, 60, \geq 3]$, $[64, 54, \geq 4]$, $[64, 44, \geq 5]$, $[64, 29, \geq 12]$, $[64, 9, \geq 15]$, when $m = 1, \ldots, 5$.

4.3. **Higher dimensional varieties.** For higher dimensional varieties, the situation is more difficult, since it is quite harder to check whether a variety contains a line (resp. a plane conic) or not.

However, Theorem A.1 in Appendix A gives some *generic* results on codes on hypersurfaces of fixed degree.

For instance, it asserts that in $\mathbf{P}^4$, almost all hypersurfaces of degree $a \geq 6$ do not contain any line, plane conic or plane cubic. Therefore, we know that codes $C_L(\Delta, G_m)^\perp$ have minimum distance $d \begin{cases} \geq m+2 & \text{if} \quad m \leq a-2 \\ \geq 2m+2 & \text{if} \quad m = a-1 \\ \geq 3m & \text{if} \quad m = a \\ > 3m & \text{if} \quad m > a \end{cases}$.

4.4. **Binary codes.** To conclude this section let us consider the case of algebraic-geometric codes over $\mathbf{F}_2$.

Theorem 4.14. *Let H be a hypersurface of $\mathbf{P}^N_{\mathbf{F}_2}$ with $N \geq 3$, let G_m be m times a hyperplane section of H and Δ be a formal sum of points avoiding the support of G_m. Then the minimum distance d of $C_L(\Delta, G_m)^\perp$ is* $\begin{cases} \geq 4 & \text{if} \quad m = 1 \\ \geq 3m & \text{if} \quad m \geq 2 \end{cases}$.

Proof. Obviously, a plane section of any hypersurface of $\mathbf{A}^N$ with $N \geq 3$ contains at most $\sharp\mathbf{A}^2(\mathbf{F}_2) = 4$ points and at most 2 of them are collinear. Therefore, since we proved that the 3 smallest kinds of configurations of points giving low weight codewords are plane configurations, Theorem 3.5 yields the result. □

5. Key tools for the proof of Theorem 3.5

In this section, we state two fundamental results for the proof of Theorem 3.5 (Lemma 5.1 and Proposition 5.2). Notice that the second one (Proposition 5.2) is not that elementary, since its proof involves the theory of residues on surfaces developped in [2].

5.1. **Context.** In the present section, m denotes an integer greater than or equal to 1. The base field k is algebraically closed, since Lemma 2.13 asserts that treating this case is sufficient.

5.2. **The statements.** The following lemma is elementary but very useful in sections 7 to 9.

Lemma 5.1. *Let $P_1, \dots, P_s$ be a minimally m–linked configuration of points in $\mathbf{P}^r$. Let d and l be two integers satisfying respectively $1 < d < m$ and $1 < l < s$. Let H be a hypersurface of degree d containing exactly l of the P_i's. Then, the $s - l$ remaining points are minimally $(m - d)$–linked.*

Proof. After a suitable reordering of the indexes, we have $P_1, \dots, P_l \in H$ and $P_{l+1}, \dots, P_s \notin H$. Assume that $P_{l+1}, \dots, P_s$ are not minimally $(m - d)$–linked. Then, after a suitable reordering of the indexes $\{l+1, \dots, s\}$, there exists a hypersurface H' of degree $m-d$ containing $P_{l+1}, \dots, P_{s-1}$ and avoiding P_s. But the hypersurface $H \cup H'$ of degree m contains $P_1, \dots, P_{s-1}$ and avoids P_s. This contradicts the assumption: "the P_i's are *minimally* m–linked". □

The following proposition gives plenty of examples of m–linked configurations of points.

Proposition 5.2. *Let a be a positive integer such that $a < m+3$. A family of $a(m+3-a)$ distinct points in $\mathbf{P}^2_k$ lying at the intersection of a curve C_1 of degree a and a curve C_2 of degree $m + 3 - a$ having no common irreducible component are m–linked.*

The proof of Proposition 5.2 will follow from the *residue formula* in the theory of residues on algebraic surfaces (see [2] Theorem 6.8). This is the reason why we give a brief review on the topic.

5.3. **Residues in dimension 2.** Let B and C be two curves embedded in a smooth surface S and intersecting themselves with multiplicity 1 at a point P. Let (u, v) be respective local equations of B and C in a neighborhood of P and ω be a rational 2-form on S of the form

$$\omega := \varphi \frac{du}{u} \wedge \frac{dv}{v},$$

where φ is a regular function in a neighborhood of P. We call 2-*residue of* ω *along* C *at* P the element

$$\mathrm{res}^2_{C,P}(\omega) := \varphi(P). \tag{R1}$$

One proves that this number does not depend on the choice of the local equations u and v. Moreover, for all regular functions f in a neighborhood of P, we have

$$\mathrm{res}^2_{C,P}(f\omega) := f(P)\varphi(P). \tag{R2}$$

In addition, assume that S is projective and let C_1, C_2 be two projective curves embedded in S and having no common component. Denote by $\mathcal{T}$ the set–theoretic intersection of C_1 and C_2. From [2] Theorem 6.8, for any rational 2–form ω on S whose pole locus is contained in $C_1 \cup C_2$, we have

$$\sum_{P \in S} \mathrm{res}^2_{C_i,P}(\omega) = \sum_{P \in \mathcal{T}} \mathrm{res}^2_{C_i,P}(\omega) = 0 \quad \text{for } i \in \{1, 2\}. \tag{R3}$$

Remark 5.3. Actually, the notion of 2–residue can be defined in a larger context, but it is irrelevant for the proof below. For references on the topic see [2] and [11].

Proof of Proposition 5.2. Denote by n the integer $a(m+3-a)$ and by $P_1, \dots, P_n$ the points lying at the intersection of C_1 and C_2. Let L be a line of $\mathbf{P}^2$ avoiding all the P_i's and x, y be affine coordinates of the affine chart $\mathbf{P}^2 \smallsetminus L$. Let f_1, f_2 be two rational functions whose divisors satisfy

$$(f_1) = C_1 - aL \qquad \text{and} \qquad (f_2) = C_2 - (m+3-a)L$$

and set

$$\omega := \frac{1}{f_1 f_2} dx \wedge dy\cdot$$

The divisor of the 2-form $dx \wedge dy$ is equal to $-3L$. Therefore, we have

$$(\omega) = mL - C_1 - C_2.$$

Notice that ω can be expressed as

$$\omega = J^{-1} \frac{df_1}{f_1} \wedge \frac{df_2}{f_2}, \quad \text{where} \quad J := \frac{\partial f_1}{\partial x}\frac{\partial f_2}{\partial y} - \frac{\partial f_2}{\partial x}\frac{\partial f_1}{\partial y}\cdot$$

Moreover, since the P_i's are distinct, the curves C_1 and C_2 have normal crossing at each P_i (it is a straightforward consequence of Bézout's theorem). Therefore, the Jacobian determinant J is nonzero at each P_i and, from (R1), we have

$$\forall i \in \{1, \dots, n\},\ \mathrm{res}^2_{C_2, P_i}(\omega) = J(P_i)^{-1}.$$

Finally, let H be a curve of degree m in $\mathbf{P}^2$ and $h(x, y)$ be an affine equation of it in $\mathbf{P}^2 \smallsetminus L$. Then, we have

$$(*) \qquad (h\omega) = H - C_1 - C_2.$$

Moreover, from (R2), we get

$$\forall i \in \{1, \dots, n\},\ \mathrm{res}^2_{C_2, P_i}(h\omega) = h(P_i) J(P_i)^{-1}.$$

From $(*)$, we have $(h\omega) \geq -C_1 - C_2$. Thus, (R3) entails

$$\sum_{i=1}^{n} \mathrm{res}^2_{C_2, P_i}(h\omega) = \sum_{i=1}^{n} J(P_i)^{-1} \mathrm{ev}_{P_i}(h) = 0.$$

This holds for all $h \in \mathcal{F}_{m,2}$ and hence gives the nontrivial linear relation in $\mathcal{F}^\vee_{m,2}$:

$$\sum_{i=1}^{n} J(P_i)^{-1} \mathrm{ev}_{P_i} = 0.$$

□

Proposition 5.2 motivates the following question.

Question 1. *Proposition 5.2 asserts that, for all $a \geq 1$ and all $m \geq 0$, a set of $a(m+3-a)$ distinct points lying at the intersection of two curves C_1 and C_2 of respective degrees a and $m+3-a$ and having no common irreducible component are m–linked. But are they minimally m–linked?*

In the end of the present section, Corollary 5.5 will give a positive answer to Question 1 when one of the curves C_1, C_2 is smooth. Afterwards, in the next sections, we will answer positively Question 1 for $a = 1, 2$ and 3, without any condition on the curves C_1, C_2. Moreover, we will prove that $m+2$ collinear points, $2m+2$ coplanar points on a conic and $3m$ points lying at the intersection of two coplanar curves of respective degrees 3 and m are the smallest configurations of minimally m–linked points **in a projective space of arbitrary dimension**. In particular, this asserts that the three

first steps of the hierarchy of minimlly m–linked points in a projective space are planar configurations.

We conclude the present section by relating the Goppa designed distance for codes on plane curves and Proposition 5.2.

5.4. **The Goppa designed distance for codes on plane curves.** Back to the case of plane curves (see the context in 4.1.1). We proved that the minimum distance of the code $C_L(D, G_m)^\perp$ is greater than or equal to the Goppa designed distance which equals $a(m+3-a)$ (see (ΔG) page 8). Therefore, the Goppa designed distance for codes on plane curves is closely related to the notion of m–linked points on the plane. In particular, we have the following result.

Theorem 5.4. *In the context of 4.1.1, assume that the degree a of the plane curve X is greater than or equal to 3. If $s = a(m+3-a)$ of the P_i's lie on a curve Y of degree $m+3-a$ which does not contain X, then these s points are minimally m–linked and the Goppa designed distance is reached for the code $C_\Omega(D, G_m)$.*

Proof. After a suitable reordering of the indexes, assume that the points $P_1, \dots, P_s$ lie at the intersection of X and Y. Obviously, by Bézout's Theorem the points $P_{s+1}, \dots, P_n$ avoid Y. From Proposition 5.2 the points $P_1, \dots, P_s$ are m–linked. Suppose that they are not minimally, then some proper subset of $\{P_1, \dots, P_s\}$ is minimally m–linked and is, from Lemma 3.3, the support of some codeword of $C_L(D, G_m)^\perp = C_\Omega(D, G_m)^\perp$. This assertion contradicts the fact that the minimum distance of $C_L(D, G_m)^\perp$ is at least equal to the Goppa designed distance, which equals s in this situation (see (ΔG) page 8). □

Corollary 5.5. *Let a be greater than or equal to 3. If $a(m+3-a)$ distinct points lie at the intersection of two curves plane curves X and Y of respective degrees a and $m+3-a$ and if one of these curves is smooth, then the points are minimally m–linked.*

6. First minimal configuration and proof of Theorem 3.8(i)

Obviously, $m+2$ collinear points of a projective space are coplanar and lie at the intersection of a line L and a plane curve C of degree $m+2$ which does not contain L. Therefore, applying Proposition 5.2 for $r = 1$, one concludes that $m+2$ collinear points are m–linked. The aim of the following lemma is to prove that they are actually *minimally* m–linked.

Context. In this section the base field k is algebraically closed (it is sufficient to treat this case thanks to Lemma 2.13) and $m \geq 0$ (even if the cases $m = 0$ and 1 are treated in 3.3.1, treating them in the present section does not make the proofs longer).

Proposition 6.1. *A set of $s \leq m+1$ distinct points $P_1, \dots, P_s \in \mathbf{P}^r$, is m–general.*

Proof. Let P_i be one of the s points. For all $j \neq i$, there exists a hyperplane containing P_j and avoiding P_i. The union of these $s-1$ hyperplanes is a surface of degree $s-1$ avoiding P_i and containing P_j for all $j \neq i$. By assumption, $s-1 \leq m$. This concludes the proof. □

The following lemma entails the converse statement of Theorem 3.8(i): *if the minimum distance of $C_L(\Delta, G_m)^\perp$ equals $m+2$, then $m+2$ of the P_i's are collinear.* Moreover, it asserts that the support of a codeword of weight $m+2$ in $C_L(\Delta, G_m)^\perp$ is a set of $m+2$ collinear points.

Proposition 6.2. *Let $P_1, \dots, P_{m+2}$ be a family of m–linked points. Then they are collinear.*

Remark 6.3. From Proposition 6.1, the P_i's in the statement of Proposition 6.2 are actually *minimally* m–linked.

Proof. Assume that the P_i's are not collinear. After a suitable reordering of the indexes, the points P_m, P_{m+1} and P_{m+2} are not collinear and hence there exists a hyperplane H containing P_{m+1}, P_{m+2} and avoiding P_m. Therefore, at least 1 and at most m of the P_i's lie out of H and, from Lemma 5.1 they are minimally $(m-1)$ linked. This yields a contradiction thanks to Proposition 7.2 applied to $m-1$. □

Let us proceed to the proof of Theorem 3.8(i).

Proof of Theorem 3.8(i). Proposition 6.1 entails that the smallest number of m–linked points in a projective space is $\geq m+2$. Proposition 5.2 entails that $m+2$ collinear points are m–linked, which yields the "if" part of Theorem 3.8(i). The "only if" part is a consequence of Proposition 6.2. □

7. Second minimal configuration and proof of theorem 3.8(ii)

Context. In this section, the ambient space is $\mathbf{P}^r$ with $r \geq 2$, the base field k is algebraically closed (see Lemma 2.13) and $m \geq 2$ (the cases $m = 0, 1$ have been treated in 3.3.1).

Lemma 7.1. *Let C be a reduced plane conic, m be a positive integer and $P_1, \ldots, P_{2m+2}$ be a family of points of C such that no $m+2$ of them are collinear. Then, there exists a plane curve C' of degree $m+1$ having no common component with C and intersecting it exactly at the points $P_1, \ldots, P_{2m+2}$.*

Proof. For all $i \in \{1, \ldots, m+1\}$, denote by L_i the line joining P_i and P_{m+1+i}. If C is irreducible, then it does not contain any line and the curve $C' := \cup_{i=1}^{m+1} L_i$ is a solution of the problem. If C is reducible, then, since no $m+2$ of the P_i's are collinear, C is a union of 2 lines D_1 and D_2 and each of these lines contains exactly $m+1$ of the P_i's. After a suitable reordering of the indexes, we have $P_1, \ldots, P_{m+1} \in D_1$ and $P_{m+2}, \ldots, P_{2m+2} \in D_2$. Then, the curve $C' := \cup_{i=1}^{m+1} L_i$ is a solution to the problem. □

From Proposition 5.2 applied to $r = 2$ and Lemma 7.1, any set of $2m+2$ points on a plane conic is m–linked. The purpose of the following proposition is to prove that it is actually *minimally* m–linked provided no $m+2$ of them are collinear.

Proposition 7.2. *A configuration of $s \leq 2m+1$ distinct points $P_1, \ldots, P_s \in \mathbf{P}^r$ such that no $m+2$ of them are collinear is m–general.*

Proof. For all $m \geq 1$, let $s_m \geq m+2$ be the smallest number of m–linked points such that no $m+2$ of them are collinear. Notice that the definition of s_m entails that an m–linked family of s_m points such that no $m+2$ of them are collinear, is actually *minimally* m–linked. We will prove that $s_m \geq 2m+2$ by induction on m.

Step 1. Initialisation: $\mathbf{m = 1}$. From lemma 3.4, we have $s_1 = 4$.

Step 2. Induction. Let $m \geq 2$ and assume that $s_{m-1} \geq 2m$. Let a_m be an integer and $P_1, \ldots, P_{a_m}$ be a family of minimally m–linked points such that no $m+2$ of them are collinear. Let c be the maximal number of collinear points in $\{P_1, \ldots, P_{a_m}\}$. Obviously, we have $2 \leq c$ and, by assumption on the P_i's, we have $c \leq m+1$.

If $\mathbf{c = m + 1}$, then there exists a hyperplane H containing $m+1$ of the P_i's and avoiding all the other ones. From Lemma 5.1, the $a_m - m - 1$ of the P_i's which lie out of H are minimally $(m-1)$–linked. Consequently, from Proposition 6.1 we have

$$a_m - m - 1 \geq m + 1 \quad \text{and hence} \quad a_m \geq 2m + 2$$

.

If $\mathbf{2 \leq c \leq m}$, then, as in the previous step, we prove that $a_m - c$ of the P_i's are minimally $(m-1)$–linked and, by definition of c, no $m+1$ of them are collinear. By induction, we have

$$a_m - c \geq s_{m-1} \geq 2m \quad \text{and hence} \quad a_m \geq 2m + 2.$$

Finally, we always have $a_m \geq 2m + 2$ and hence $s_m \geq 2m + 2$. □

The following corollary will be useful in what follows.

Corollary 7.3. *Let $m \geq 2$ and $P_1, \ldots, P_s$ be a minimally m–linked configuration of points with $s \leq 2m + 1$. Then, $s = m + 2$ and the P_i's are collinear*

Proof. Since the P_i's are m–linked and $s \leq 2m + 1$, then $m + 2$ of them are collinear. Indeed, if not, this would contradict Proposition 7.2. Thus, $m+2$ of the P_i's are m–linked and hence $s = m + 2$ since the P_i's are supposed to be minimally m–linked. □

The following proposition yields the converse statement of Theorem 3.8(ii): *if the minimum distance d of $C_L(\Delta, G_m)^\perp$ equals $2m+2$, then no $m+2$ of the P_i's are collinear and $2m+2$ of them lie on a plane conic.* Moreover, it asserts that if $d = 2m+2$, then the support of a minimum weight codeword of $C_L(\Delta, G_m)^\perp$ is contained in a plane conic.

Proposition 7.4. *An m–linked configuration of $2m + 2$ points such that no $m + 2$ of them are collinear is a family of points lying on a plane conic.*

Remark 7.5. As in Remark 6.3, Proposition 7.2 entails that the points in the above statement are actually *minimally* m–linked.

To prove Proposition 7.4, we need Lemma 7.6 below. This Lemma will actually be also useful in Section 9.

Lemma 7.6. *For all $m \geq 1$, any minimally m–linked configuration of $t \leq 3m$ points is a set of coplanar points.*

Proof. Let $m \geq 1$ and $t \leq 3m$. Let $P_1, \ldots, P_t$ be a set of minimally m-linked points and assume that they are not coplanar. Let r be the maximal number of coplanar points in $\{P_1, \ldots, P_t\}$. By assumption, we have $r < t$ and obviously, $r \geq 3$.

Claim 1: Some set of $t - r$ of the P_i's is minimally $(m-1)$–linked. Indeed, by definition of r, there exists a hyperplane containing r of the P_i's and avoiding the $t - r$ other ones. From Lemma 5.1, these $t - r$ points are minimally $(m-1)$–linked.

We will prove the result by induction on m.

If $\mathbf{m = 1}$, then it is obvious: 3 points are always coplanar.

Let $\mathbf{m \geq 2}$ and assume the property to be true for all $1 \leq k < m$. From Claim 1, $t - r$ of the P_i's, say $P_{r+1}, \ldots, P_t$, are minimally $(m-1)$–linked. Since $r \geq 3$, we have $t - r \leq 3m - 3$ and, by induction, the points $P_{r+1}, \ldots, P_t$ are coplanar. Therefore, using the very same argument as in Claim 1, one proves that the coplanar points $P_1, \ldots, P_r$

are also minimally $(m-1)$–linked. Thus, from Proposition 6.1 (applied to $m-1$), we have $r \geq m+1$ and $t-r \geq m+1$. Since $t \leq 3m$, the previous inequalities yield:

$$2m-1 \geq r \geq m+1.$$

However, since $P_1, \ldots, P_r$ are minimally $(m-1)$–linked and $r \leq 2m-1$, Corollary 7.3 yields $r = m+1$ and $P_1, \ldots, P_r$ are collinear. Therefore, at least $m+2$ of the P_i's are coplanar, which contradicts $r = m+1$. □

Now, let us proceed to the proof of Proposition 7.4.

Proof of Proposition 7.4. Let $P_1, \ldots, P_{2m+2}$ be points satisfying the hypotheses of Proposition 7.4. From Remark 7.5 the P_i's are actually minimally m–linked and, from Lemma 7.6, they are coplanar. There remains to prove that they lie on a conic.

Let us consider separately the cases $m = 1$ and $m = 2$. If $m = 1$, then it is obvious: 4 coplanar points are always 1–linked and lie on a plane conic. If $m = 2$, then 6 points of $\mathbf{P}^2$ which do not lie on a conic are in 2–general position. Indeed, any 5 of them lie on a conic avoiding the 6th one.

From now on, $m \geq 3$. Let L be a line containing a maximal number of the P_i's. By assumption, it contains at most $m+1$ of them. Let us consider three distinct cases.

Case 1. Assume that L contains $m+1$ of the P_i's. From Lemma 5.1, the $m+1$ remaining points are minimally $(m-1)$–linked. Therefore, from Proposition 6.2 these points are collinear and the P_i's lie on a reducible conic.

Case 2. Assume that L contains m of the P_i's. Then no $m+1$ of the $m+2$ remaining points are collinear. By assumption, $m \geq 3$ and hence $2m+1 \geq m+2$. Therefore, from Proposition 7.2 (applied to $m-1$), the $m+2$ remaining points are in $(m-1)$–general position. However, using the same reasoning as in Case 1, it can be shown that these points are minimally $(m-1)$–linked. Consequently, this situation never happens.

Case 3. Assume that L contains at most $m-1$ points. Let C be a conic containing at least 5 of the P_i's, say P_1, P_2, P_3, P_4, P_5 and assume that C avoids at least one of the P_i's, say P_{2m+2}. By assumption on L, no m of the P_i's out of C are collinear. Thus, from Proposition 7.2 (applied to $m-2$), the P_i's out of C are in $(m-2)$–general position. However, from Lemma 5.1 they are minimally $(m-2)$–linked. Consequently, the P_i's all lie on C. □

Let us proceed to the proof of Theorem 3.8(ii).

Proof of Theorem 3.8(ii). From Proposition 7.2, the smallest number of m–linked points such that no $m+2$ are collinear is $\geq 2m+2$. It is actually an equality from Proposition 5.2 since $2m+2$ points on a plane conic are m–linked. This gives the "if" part of the statement. The "only if" part is a consequence of Proposition 7.4. □

8. Third minimal configuration and proof of theorem 3.8(iii)

From Proposition 5.2, we know that $3m$ coplanar points lying at the intersection of a cubic and a curve of degree m having no common component are m–linked. The aim of the following proposition is to prove that they are actually *minimally* m–linked.

Context. The ambient space is $\mathbf{P}^r$ with $r \geq 2$, the base field k is algebraically closed and $m \geq 1$ (even if the cases $m = 0, 1$ have been treated in 3.3.1, keeping the case $m = 1$ does not make the proofs longer).

Proposition 8.1. *Any $s \leq 3m - 1$ distinct points such that no $m + 2$ of them are collinear and no $2m + 2$ of them lie on a plane conic are m–general.*

To prove Proposition 8.1, we need the following elementary lemma.

Lemma 8.2. *Let C be a plane conic contained in $\mathbf{P}^r$ and $P_1, \ldots, P_n$ be points avoiding C. Then, there exists a hypersurface of degree 2 containing C and avoiding all the P_i's.*

Proof. If $r = 2$ it is obvious, the expected hypersurface is C. If $r \geq 3$, then consider the set of 3–codimensional linear subspaces $\Pi \subset \mathbf{P}^r$ such that the cone generated by C over Π is a hypersurface of degree 2 and avoids the P_i's. One proves easily that this set corresponds to a nonempty open subset of the Grassmanian $\mathrm{Grass}(r-2, k^{r+1})$ (see [12] I.4.1 example 1 for a definition). □

Let us prove Proposition 8.1.

Proof of Proposition 8.1. The method is nearly the same as that of the proof of Proposition 7.2. For all $m \geq 1$, denote by t_m be the smallest cardinal of an m–linked set of points such that no $2m + 2$ of them lie on a plane conic and no $m + 2$ of them are collinear. It is worth noticing that, by definition of t_m, such an m–linked set of t_m points is actually *minimally* m–linked.

To prove the proposition, we have to prove that $t_m \geq 3m$ for all $m \geq 1$. We will prove it by induction on m.

Step 1. Initialisation. Proposition 7.2 applied to $m = 1$ and $m = 2$ respectively entails $t_1 > 3$ and $t_2 \geq 6$. From the same Proposition applied to $m = 3$, any $s \leq 7$ points such that no 5 of them are collinear are m–general. Thus, $t_3 \geq 8$. Moreover, from Proposition 7.4, 8 points such that no 5 of them are collinear and which do not lie on a plane conic are not m–linked and hence are m–general. Thus, $t_3 \geq 9$.

Step 2. Induction. Let m be greater than or equal to 4, let a_m be an integer and $P_1, \ldots, P_{a_m}$ be a minimally m–linked configuration of points such that no $m+2$ of them are collinear and no $2m+2$ of them lie on a plane conic. From Proposition 7.2, we have $a_m \geq 2m + 2$. Moreover, by assumption on the P_i's, since no $2m + 2$ of them lie on a conic, from Proposition 7.4, we have $a_m \neq 2m + 2$ and hence

$$(\clubsuit) \qquad a_m > 2m + 2$$

Let c be the maximal number of collinear points in $\{P_1, \ldots, P_{a_m}\}$ and d be the maximal number of the P_i's lying on a plane conic. Obviously, we have $2 \leq c$ and $5 \leq d$. Moreover, by assumption on the P_i's, we have

$$c \leq m + 1 \quad \text{and} \quad d \leq 2m + 1.$$

We will consider separately some particular values of c and d.

Case 2.1. If $d \geq 2m$, then let C be a conic containing d of the P_i's. From Lemma 8.2, there exists a hypersurface of degree 2 containing C and avoiding all the points out of it. From Lemma 5.1, the $a_m - d$ remaining points are $(m-2)$–linked. Thus, from Proposition 6.1, we have

$$a_m - d \geq m \quad \text{and hence} \quad a_m \geq 3m.$$

Case 2.2. If $c = m+1$ and $d \leq 2m-1$, then let L be a line containing $m+1$ of the P_i's. There exists a hyperplane H containing L and avoiding all P_i's out of L. Consequently, from Lemma 5.1, the $a_m - m - 1$ of the P_i's lying out of L are minimally $(m-1)$–linked. Let us consider separately two different situations.

(a) If $m+1$ of these points out of L lie on a line L', then one proves by the same reasoning that the $a_m - 2m - 2$ of the P_i's lying out of $L \cup L'$ are minimally $(m-2)$–linked. Consequently, from Proposition 6.1 applied to $m-2$, we have

$$a_m - 2m - 2 \geq m, \quad \text{which entails} \quad a_m \geq 3m + 2 \geq 3m.$$

(b) If no $m+1$ of the points out of L are collinear, then, from Proposition 7.2, we have

$$a_m - m - 1 \geq 2m \quad \text{and hence} \quad a_m \geq 3m + 1 \geq 3m.$$

Case 2.3. If $3 \leq c \leq m$ and $d \leq 2m-1$, then, one proves as in Case 2(b) that $a_m - c$ of the P_i's are minimally $(m-1)$–linked. Moreover, by definition of c and d, no $m+1$ of these $a_m - c$ points are collinear and no $2m$ of them lie on a plane conic. The induction hypothesis yields

$$a_m - c \geq t_{m-1} \geq 3m - 3 \quad \text{and hence} \quad a_m \geq 3m.$$

Case 2.4. If $c = 2$, $d \leq 2m-1$ and the P_i's are not coplanar, then there exists a hyperplane H containing at least 3 of the P_i's and avoiding at least 1 of them. Let $h \geq 3$ be the number of P_i's contained in H. From Lemma 5.1, the points out of H are minimally $(m-1)$–linked and, as in the previous case, the induction hypothesis yields

$$a_m - h \geq t_{m-1} \quad \text{and hence} \quad a_m \geq 3m.$$

From now on, the P_i's are assumed to be coplanar. Therefore, we always have $d \geq 5$.

Case 2.5. If $c = 2$, $2m-2 \leq d \leq 2m-1$ and the P_i's are coplanar, then let C be a conic containing d of the P_i's. From Lemma 5.1, the points out of C are $(m-2)$–linked and no 3 of them are collinear (since $c = 2$). Thus, from Proposition 7.4, we have

$$a_m - d \geq 2m - 2, \quad \text{which entails} \quad a_m \geq 4m - 4$$

and, since $m \geq 4$, this entails $a_m \geq 3m$.

Case 2.6. If $c = 2$, $6 \leq d \leq 2m-3$ and the P_i's are coplanar, then let C be a conic containing d of the P_i's. From Lemma 5.1, the points lying out of C are minimally $(m-2)$–linked. Moreover, by assumption on c and d, no 3 of these points are collinear and no $2m-2$ of them lie on a conic. By the induction hypothesis for $m-2$, we have

$$a_m - d \geq t_{m-2} \geq 3m - 6, \quad \text{thus} \quad a_m \geq 3m.$$

Case 2.7. If $c = 2$, $d = 5$ and the P_i's are coplanar but do not lie on a cubic curve, then let C be a cubic curve containing at least 9 of the P_i's. Such a curve exists since the linear system of plane cubics has dimension 9. By assumption, C avoids at least one of the P_i's. Denote by r the number of the P_i's contained in C. We have $9 \leq r < a_m$ and, from Lemma 5.1, the $a_m - r$ of the $P_i's$ lying out of C are minimally $(m-3)$–linked. Moreover, by assumption on c and d, no 3 of these remaining points are collinear and no 6 of them lie on a cubic. Since $m \geq 4$, we have $(m-3)+2 \geq 3$ and $2(m-3)+2 \geq 6$. Thus, by the induction hypothesis for $m-3$, we have

$$a_m - r \geq t_{m-3}, \quad \text{which entails} \quad a_m \geq 3m - 9 + r \geq 3m.$$

Case 2.8. If $c = 2$, $d = 5$ and the P_i's lie on a plane cubic curve, then let C be this cubic curve. Notice that, by assumption, $m \geq 4$ and, from (♣), we have $a_m \geq 2m + 3$ and hence $a_m \geq 11$. Since no 3 of the P_i's are collinear and no 6 of them lie on a conic and

$a_m \geq 11$, one proves easily that C is irreducible. Then, $a_m \geq 3m$ as a straightforward consequence of Lemma 8.3 below.

Conclusion. In all the considered cases, we have $a_m \geq 3m$. Thus, $t_m \geq 3m$. □

Lemma 8.3. *Let m be an integer greater than or equal to 3. Let $P_1, \ldots, P_{3m-1} \in \mathbf{P}^2$ be a family of points lying on an irreducible plane cubic curve C such that no 3 of them are collinear and no 6 of them lie on a conic. Then, the P_i's are in m–general position.*

Proof. Let F_C be an homogeneous equation of C. Let us introduce some facts and notations on linear systems. Denote by E_m the subspace of $\mathcal{F}_{m,2}$ of homogeneous forms vanishing on C (i.e. $E_m := \mathcal{F}_{m-3,2}F_C$). Choose a subspace $H_m \subset \mathcal{F}_{m,2}$ such that $\mathcal{F}_{m,2} = E_m \oplus H_m$ and let Γ_m be the linear system $\mathbf{P}(H_m)$. It is a linear system of curves of degree m which do *not* contain C. Its dimension is

$$(\spadesuit) \qquad \dim(\Gamma_m) = \dim(\mathcal{F}_{m,2}) - \dim(\mathcal{F}_{m-3,2}) - 1 = 3m - 1.$$

Let us prove the m–generality of $P_1, \ldots, P_{3m-1}$ by induction on m.

Step 1. Initialisation. If $m = 3$, then consider 8 points of a plane cubic curve C. Since no 3 of them are collinear and no 6 lie on a conic, from [5] Proposition V.4.3, the linear system of cubic containing 7 of them has no other base point. Thus, the points are in 3-general position.

Step 2. Induction. Let $m \geq 4$ and assume the induction hypothesis to be true for $m - 1$. By symmetry on the indexes, to prove the result, it is sufficient to prove the existence of a curve of degree m containing $P_1, \ldots, P_{3m-2}$ and avoiding P_{3m-1}. We will prove the existence of a curve D of degree $(m - 1)$ containing $P_3, \ldots, P_{3m-2}$, and avoiding P_{3m-1}. By assumption no 3 of the P_i's are collinear and hence the line L joining P_1 and P_2 avoids P_{3m-1}. Consequently, the curve $L \cup D$ of degree m will avoid P_{3m-1} and contain all the other P_i's.

Sub-step 2.1 Let j be an integer in $\{1, 2, 3\}$. By induction, the points $P_j, P_4, \ldots, P_{3m-2}$ are in $(m-1)$–general position. Therefore, the maps $\mathrm{ev}_{P_j}, \mathrm{ev}_{P_4}, \ldots, \mathrm{ev}_{P_{3m-2}}$ are linearly independent in $\mathcal{F}^\vee_{m-1,2}$ and, since they all vanish on E_{m-1} (recall that E_{m-1} denotes the space of forms of degree $m - 1$ vanishing on C), they induce independent maps in $(\mathcal{F}_{m-1,2}/E_{m-1})^\vee \cong H^\vee_{m-1}$. Let Λ_j be the maximal sub-system of Γ_{m-1} of curves containing $P_j, P_4, \ldots, P_{3m-2}$. From ($\spadesuit$) and since $\mathrm{ev}_{P_j}, \mathrm{ev}_{P_4}, \ldots, \mathrm{ev}_{P_{3m-2}}$ are linearly independent in $H^\vee_{m-1}$,we have

$$\dim(\Lambda_j) = \dim(\Gamma_{m-1}) - (3m - 4) = 0.$$

Sub-step 2.2 For all $j \in \{1, 2, 3\}$, denote by D_j the single element of Λ_j. It is the only element in Γ_{m-1} containing the points $P_j, P_4, \ldots, P_{3m-2}$. For the very same reason, there exists a unique element $D_{3m-1} \in \Gamma_{m-1}$ containing the points $P_4, \ldots, P_{3m-1}$.

Let us prove that at least one of the curves D_1, D_2, D_3 avoids P_{3m-1}. Assume the negation of the statement, i.e. "P_{3m-1} lies on D_1, D_2 and D_3". Since D_{3m-1} is the unique element of Γ_{m-1} containing $P_4, \ldots, P_{3m-1}$, this entails $D_1 = D_2 = D_3 = D_{3m-1}$ and this curve meets C at at least $3m - 1$ points. But such a situation contradicts Bézout's theorem. Thus, for a suitable ordering of the indexes $1, 2, 3$, the curve D_3 avoids P_{3m-1}, which concludes the proof. □

To conclude the present section, let us state the following corollary of Proposition 8.1, which can be regarded as a generalisation of Corollary 7.3.

Corollary 8.4. *Let m, n be two integers satisfying $m \geq 3$ and $n \leq 3m-1$. Let $P_1, \ldots, P_n$ be a minimally m–linked configuration of points in a projective space, then we have either $n = m+2$ and the P_i's are collinear or $n = 2m+2$ and the P_i's lie on a plane conic.*

Proof. Since the P_i's are not in m–general position, from Proposition 8.1, we have either $m+2$ of them are collinear or $2m+2$ of them lie on a plane conic. If $m+2$ of the P_i's are collinear, then, since the P_i's are *minimally* m–linked, there cannot be other points in addition to the $m+2$ collinear points and hence $n = m+2$. For the very same reasons, if $2m+2$ of them lie on a plane conic, then $n = 2m+2$. □

9. End of the proof of theorem 3.8

Context. The ambient space is $\mathbf{P}^r$ with $r \geq 2$, the base field k is algebraically closed and $m \geq 3$ (because of Remark 3.6).

Proposition 9.1. *An m–linked configuration of $3m$ points such that no $m+2$ of them are collinear and no $2m+2$ of them lie on a plane conic is a family of coplanar points lying at the intersection of a cubic and a curve of degree m having no common component.*

Remark 9.2. As in Remarks 6.3 and 7.5, the $3m$ points in the statement of Proposition 9.1 are, from Proposition 8.1, *minimally* m–linked.

For the proof of proposition 9.1, we need Lemmas 9.3 and 9.4.

Lemma 9.3. *Let n be an integer greater than of equal to 6 and $P_1, \ldots, P_n$ be a family of coplanar points which do not lie on a conic. Then, there exists 6 of them which do not lie on a conic.*

Proof. **Step 1.** Let us prove that 5 of the P_i's are in 2–general position. Proposition 7.2 asserts that 5 coplanar points are 2–general if no 4 of them are collinear. Since the P_i's do not lie on a conic, they are not collinear. Therefore, one can reorder the indexes such as P_1, P_2 and P_3 are not collinear. For all pairs of distinct integers $i, j \leq n$, denote by $L_{i,j}$ the line joining P_i and P_j. Now we have to prove that there exists two of the P_i's with $i > 3$ which do not both lie on one of the lines $L_{1,2}, L_{1,3}$ and $L_{2,3}$. If not, then the points $P_4, \ldots, P_n$ would all lie on one of the lines $L_{1,2}, L_{1,3}$ and $L_{2,3}$, say $L_{1,2}$. However, this entails that the P_i's would all lie on the conic $L_{1,2} \cup L_{2,3}$, which yields to a contradiction.

Step 2. From the previous step, after a suitable reordering of the indexes, the points $P_1, \ldots, P_5$ are in 2–general position and the dimension of the linear system of conics in $\mathbf{P}^2$ has dimension 5, there exists a unique conic C containing $P_1, \ldots, P_5$. By assumption on the P_i's, C avoids at least one of P_i's, say P_6 (after a suitable reordering of the indexes). Thus, the points $P_1, \ldots, P_6$ do not lie on a conic. □

Lemma 9.4. *A minimally m–linked family of $3m$ coplanar points such that no $m+2$ of them are collinear and no $2m+2$ of them lie on a conic, lies on a cubic curve.*

Proof. Let $P_1, \ldots, P_n$ be such a configuration of points. To prove the result, we have to treat separately the cases $m = 3$ and 4.

Step 1. Small values of m. If $m = 3$, then it is obvious since 9 coplanar points always lie on a cubic. If $m = 4$, then, since the P_i's are not assumed to be collinear, after a suitable reordering of the indexes, P_1, P_2 and P_3 are not collinear. Let C be a cubic curve containing the points $P_4, \ldots, P_{12}$. If some of the points P_1, P_2, P_3 lie out of C, then, from Lemma 5.1, they are minimally 1–linked. Thus, from Proposition 6.1, their

number is 3 and, from Proposition 6.2, they are collinear, which yields a contradiction. Thus, all the P_i's lie on C.

Step 2. Other values of m. From now on, assume that $m \geq 5$ and that the P_i's do not lie on a cubic. Let r be the maximal number of the P_i's which are contained in a plane cubic curve. Obviously, we have $r \geq 9$ and, by assumption on the P_i's, we have $r < 3m$.

Sub-step 2.1. If $r = 9$, then a cubic curve containing 9 of the P_i's always avoids all the other ones. Let s, t be the integers satisfying

$$m = 3s + t, \quad \text{with} \quad s \geq 1 \quad \text{and} \quad t \in \{1, 2, 3\}.$$

Since $r = 9$, given any family of $9s$ elements of $\{P_1, \ldots, P_{3m}\}$, one can construct s cubic curves whose union contains all of the $9s$ elements of this family and avoids all the $3t$ other P_i's. Thanks to Lemma 5.1, it entails that any family of $3t$ elements of $\{P_1, \ldots P_{3m}\}$ is minimally t–linked. Now, let us consider the three situations given by the three different possible values of t. We will get a contradiction in these three cases.

(a) If $t = 1$, then, since the P_i's are not collinear, there exists a 3–uplet of them which are not collinear and hence not 1–linked.
(b) If $t = 2$, then, since the P_i's do not lie on a conic and from Lemma 9.3, one can choose 6 of the P_i's which do not lie on a conic. Therefore, there exists a conic containing 5 of these 6 points and avoiding the 6th one, contradicting the fact that these 6 points are minimally 2–linked.
(c) If $t = 3$. Since $r = 9$, one can prove that 9 of the P_i's are always in 3–general position. Indeed, if $P_1, \ldots, P_9$ were 3–linked, then, from Lemma 2.5(v), the maximal linear system of cubic curves containing $P_1, \ldots, P_9$ would have dimension greater than or equal to 1. Thus, there would exist a cubic containing these 9 points and a 10th one, contradicting the assumption "$r = 9$".

Sub-step 2.2. If $r > 9$, then let C be a cubic containing r of the P_i's. From Lemma 5.1, the $3m - r$ points out of C are minimally $(m-3)$–linked. Since $3m - r < 3(m-3)$, from Corollary 8.4 applied to $m - 3$, we have either $3m - r = m - 1$ and the P_i's out of C are collinear or $3m - r = 2m - 4$ and the P_i's out of C lie on a plane conic. Let us treat separately these two situations.

Case 2.2.1. If $3m - r = m - 1$ *and the* P_i*'s out of* C *are collinear*, then denote by L the line containing the P_i's lying out of C. The line L contains at least $m - 1$ of the P_i's and hence avoids at most $2m - 1$ of them. From Lemma 5.1, the P_i's lying out of L are minimally $(m-1)$–linked. Since $m \geq 5$, we have $2m - 1 \leq 3m - 4$ and hence, the number of the P_i's lying out of L is lower than or equal to $3m - 4$. Therefore, from Corollary 8.4 applied to $m - 1$, the P_i's out of L lie either on a conic or on a line. But both assertions contradict the assumption: *"the* P_i*'s do not lie on a cubic"*.

Case 2.2.2. If $3m - r = 2m - 4$ *and the* P_i*'s out of* C *lie on a conic*, then denote by Q this conic. From Lemma 5.1, the $r = m + 4$ points lying out of Q (and hence on C) are minimally $(m-2)$–linked. Thus, from Corollary 8.4, they lie on a conic Q' and $r = m + 4 = 2m - 2$. Therefore, $m = 6, r = 10$ and Q' contains 10 of the P_i's. Let L be a line containing at least one of the P_i's out of Q', then the cubic $Q' \cup L$ contains at least 11 of the P_i's, which contradicts "$r = 10$". □

Now, let us prove Proposition 9.1

Proof of Proposition 9.1. Let $P_1, \ldots, P_{3m}$ be an m–linked configuration of points such that no $m + 2$ of them are collinear and no $2m + 2$ lie on a plane conic. From Remark

9.2, these points are actually minimally m–linked. From Lemma 7.6, they are coplanar and from Lemma 9.4, they lie on a cubic C. There remains to prove that they lie at the intersection of C with a curve of degree m having no common component with C.

To prove this, we will use similar objects as in the proof of Lemma 8.3. Let F_C be a homogeneous equation of C. Let E_m be the subspace of $\mathcal{F}_{m,2}$ of homogeneous forms vanishing on C and let H_m be a complement subspace of E_m in $\mathcal{F}_{m,2}$, that is $\mathcal{F}_{m,2} = E_m \oplus H_m$. Let Γ_m be the linear system $\Gamma_m := \mathbf{P}(H_m)$. It is a linear system of curves of degree m not containing C. From (♠) page 21, we have

$$\dim(\Gamma_m) = 3m - 1.$$

Consequently, there exists an element D of Γ_m containing the points $P_1, \ldots, P_{3m-1}$. Moreover, the curve cannot avoid P_{3m} since the P_i's are minimally m–linked. There remains to prove that D has no common component with C.

If C is irreducible, then it is obvious since the elements of Γ_m do not contain C.

If C is reducible, then $C = C_1 \cup C_2$ such that C_1 is a line and C_2 a conic (possibly reducible).

By assumption, at most $m+1$ of the P_i's lie on C_1 and at most $2m+1$ of them lie on C_2. Afterwards, from Lemma 5.1, the P_i's lying out of C_1 (resp. C_2) are minimally $(m-1)$–linked (resp. $(m-2)$) and, from Lemma 8.4, their number is $2m$ (resp. m). Finally, after a suitable ordering of the indexes, $P_1, \ldots, P_m \in C_1$ and $P_{m+1}, \ldots, P_{3m} \in C_2$. Moreover, none of the P_i's lie on $C_1 \cap C_2$.

Suppose that $C_1 \subset D$ and C_2 has no common component with D. Then $D = C_1 \cup D_1$ where D_1 has degree $m-1$. Since none of the P_i's lie on $C_1 \cap C_2$, the points $P_{m+1}, \ldots, P_{3m}$ lie on $C_2 \cap D'$, but this contradicts Bézout's Theorem.

Conversely, if $C_2 \subset D$ and C_1 has no common component with D, then almost the same reasoning leads also to a contradiction. □

We are now able to conclude the proof of Theorem 3.8 by proving items (iii) and (iv).

Proof of Theorem 3.5(iii). From Proposition 8.1 the smallest number of m–linked points such that no $m+2$ are collinear and no $2m+2$ lie on a plane conic is $\geq 3m$. From Proposition 5.2, this inequality is actually an equality since $3m$ points lying at the intersection of two coplanar curves of respective degrees 3 and m are m–linked. This yields the "if" part of Theorem 3.8(iii). The "only if" part is a consequence of Proposition 9.1. Item (iv) is a straightforward consequence of (i), (ii) and (iii). □

Conclusion

Using the notion of m–generality and in particular that of *being minimally m–linked*, we have obtained some results on the minimum distance of duals of arbitrary dimensional algebraic–geometric codes. For plane curves, these results improve in some situations the well-known Goppa bound. They also give a method to cleverly puncture such a code on a plane curve in order to drastically increase its dual minimum distance.

Even if the proofs are long and sometimes technical, they make worthy the notion of "being minimlly m–linked". This notion appears to be powerful and easy to handle.

To obtain results on dual algebraic–geometric codes, we described the three first items of the hierarchy of minimally m–linked configurations of points in a projective space. To improve Theorem 3.5 it would be interesting to find further items of this hierarchy. Notice that these first items correspond to configurations of coplanar points. Nevertheless, the following ones could correspond, for points in $\mathbf{P}^N$, where $N \geq 3$, to non coplanar configurations of points.

Acknowledgements

I would like to thank Marc Perret and Daniel Augot for their relevant comments about this article. Computations in Section 4 have been made thanks to the software Magma.

Appendix A. Varieties not containing plane curves of low degree

From Theorem 3.5, to get good codes of the form $C_L(\Delta, G)^{\perp}$, it is interesting to look for varieties which do not contain any plane curves of degree $1, 2$ and 3. The following result makes possible to check whether a "generic" hypersurface of $\mathbf{P}^N$ with fixed degree contains any line, plane conic or plane cubic. The proof is pretty elementary and uses the same tools as that of [12] Theorem I.6.4.10. We give it because of a lack of references.

Theorem A.1. *Let N, d, r be integers such that $N \geq 3$, $d \geq 2$ and $d \geq r \geq 1$. Then, almost all hypersurfaces of degree d in $\mathbf{P}^N$ do not contain any plane curve of degree r if*

$$\binom{d+2}{2} - \binom{d-r+2}{2} - x_{r,N} > 0,$$

where

$$x_{r,N} = \begin{cases} 2N-2 & \text{if } r = 1 \\ \binom{r+2}{2} + 3N - 7 & \text{if } r > 1 \end{cases}.$$

Remark A.2. The condition of the theorem is sufficient but not necessary. For instance, for $N = 3$ and $r = 3$, we get: *almost all surfaces of $\mathbf{P}^3$ of degree ≥ 5 do not contain any plane cubic.* Actually, it is also true for surfaces of degree 4. Indeed, for $N = 3$, $r = 4$ and $r = 1$ the theorem asserts that generic surfaces of degree 4 do not contain any line. Moreover, it is easy to check that a surface of degree 4 which does not contain any line cannot contain any plane cubic (consider the plane sections of such a surface).

Proof. **Notations.** In this proof, for all integers d, N, we denote by $\Gamma_{d,N}$ the linear system $\mathbf{P}(\mathcal{F}_{d,N})$ of hypersurfaces of degree d in $\mathbf{P}^N$. Moreover, for all $r \geq 1$, denote by $X_{r,N}$, the variety parametrising the set of the plane curves of degree r contained in $\mathbf{P}^N$ and by $V_{r,d,N}$ the variety defined by

$$V_{r,d,N} := \{(C, H) \in X_{r,N} \times \Gamma_{d,N} \mid C \subset H\}.$$

Step 1. The variety of lines in $\mathbf{P}^N$: the case $\mathbf{r = 1}$. For all $N \geq 2$, the variety $X_{1,N}$ is isomorphic to the Grassmanian $\mathrm{Grass}(2, k^{N+1})$. Thus,

$$\dim X_{1,N} = 2N - 2.$$

(see [12] I.4.1 example 1).

Step 2. The variety of planes curves of degree $\mathbf{r \geq 2}$ in $\mathbf{P}^N$. For all $N \geq 2$, the variety parametrising the planes contained in $\mathbf{P}^N$ is isomorphic to the Grassmanian $\mathrm{Grass}(3, k^{N+1})$. This variety has dimension $3N - 6$. Then, for all $r \geq 2$, the variety $X_{r,N}$ is a $\Gamma_{r,2}$–bundle over $\mathrm{Grass}(3, k^{N+1})$ and hence has dimension

$$\dim X_{r,N} = \binom{r+2}{2} + 3N - 7.$$

Step 3. Consider the following diagram

$$\begin{tikzcd}
V_{r,d,N} \arrow[dr] \arrow[drr, bend left, "\varphi_1"] \arrow[ddr, bend right, "\varphi_2"'] & & \\
& X_{r,N} \times \Gamma_{d,N} \arrow[r, "\pi_1"] \arrow[d, "\pi_2"'] & X_{r,N} \\
& \Gamma_{d,N} &
\end{tikzcd}$$

where π_1 and π_2 denote the canonical projections. To prove the theorem, we have to prove that φ_2 is not dominant. Thus, it is sufficient to prove that $\dim(V_{r,d,N}) < \dim \Gamma_{d,N}$.

Let us compute the dimension of $V_{r,d,N}$. Notice that, for a given plane curve C of degree r in $\mathbf{P}^N$, the set of hypersurfaces of degree d containing C is parametrised by some projective space $\mathbf{P}^l$ whose dimension l does not depend on C. Therefore, $V_{r,d,N}$ is a $\mathbf{P}^l$–bundle over $X_{r,N}$. Since we know the dimension of $X_{r,N}$, we just have to compute the dimension l of the fibre $F_{r,d,N}$ of φ_1.

Let C be a plane curve of degree r in $\mathbf{P}^N$ and let Π be the plane containing it. Consider the map

$$\nu : \mathcal{F}_{d,N} \twoheadrightarrow \mathcal{F}_{d,2}$$

which sends a form of degree d to its restriction to Π. The set of forms of degree d in $\mathcal{F}_{d,2}$ vanishing on C is isomorphic to $\mathcal{F}_{d-r,2}$. Therefore, the fibre $F_{r,d,N}$ satisfies

$$F_{r,d,N} \cong \mathbf{P}(\nu^{-1}(\mathcal{F}_{d-r,2})).$$

The dimension of $F_{r,d,N}$ is

$$\dim F_{r,d,N} = \dim \mathcal{F}_{d-r,2} + \dim \mathcal{F}_{d,N} - \dim \mathcal{F}_{d,2} - 1.$$

Finally, we have

$$\dim \Gamma_{d,N} - \dim V_{r,d,N} = \binom{d+2}{2} - \binom{d-r+2}{2} - \dim X_{r,N}.$$

□

References

[1] Y. Aubry. Reed-Muller codes associated to projective algebraic varieties. In *Coding theory and algebraic geometry (Luminy, 1991)*, volume 1518 of *Lecture Notes in Math.*, pages 4–17. Springer, Berlin, 1992.

[2] A. Couvreur. Sums of residues on algebraic surfaces and application to coding theory. To appear in *Journal of Pure and Applied Algebra*.

[3] A. Couvreur. *Résidus de 2-formes différentielles sur les surfaces algébriques et applications aux codes correcteurs d'erreurs*. PhD thesis, Institut de Mathématiques de Toulouse, Université Paul Sabatier, France, `http://iml.univ-mrs.fr/~couvreur/english/research.html#publi`, 2008.

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

[5] R. Hartshorne. *Algebraic geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1977.

[6] J. Kollàr, K. E. Smith, and A. Corti. *Rational and nearly rational varieties*, volume 92 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2004.

[7] G. Lachaud. Projective Reed-Muller codes. In *Coding theory and applications (Cachan, 1986)*, volume 311 of *Lecture Notes in Comput. Sci.*, pages 125–129. Springer, Berlin, 1988.

[8] G. Lachaud. Number of points of plane sections and linear codes defined on algebraic varieties. In *Arithmetic, geometry and coding theory (Luminy, 1993)*, pages 77–104. de Gruyter, Berlin, 1996.

[9] J. B. Little. Algebraic geometry codes from higher dimensional varieties, 2008. Preprint, arXiv:math/0802.2349v1.

[10] D. Mumford. *Lectures on curves on an algebraic surface*. With a section by G. M. Bergman. Annals of Mathematics Studies, No. 59. Princeton University Press, Princeton, N.J., 1966.

[11] A. N. Paršin. On the arithmetic of two-dimensional schemes. I. Distributions and residues. *Izv. Akad. Nauk SSSR Ser. Mat.*, 40(4):736–773, 949, 1976.

[12] I. R. Shafarevich. *Basic algebraic geometry. 1*. Springer-Verlag, Berlin, second edition, 1994.

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

[14] S. G. Vlăduts and Y. I. Manin. Linear codes and modular curves. In *Current problems in mathematics, Vol. 25*, Itogi Nauki i Tekhniki, pages 209–257. Akad. Nauk SSSR Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1984.

[15] F. Voloch and M. Zarzar. Algebraic geometric codes on surfaces, 2005. Preprint. `http://www.ma.utexas.edu/users/voloch/Preprints/luminy.pdf`.

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

INRIA Saclay - École polytechnique, Laboratoire d'informatique (LIX), 91128 Palaiseau Cedex, France

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