Journal of Pure and Applied Algebra 217 (2013) 269–279

Contents lists available at SciVerse ScienceDirect

Journal of Pure and Applied Algebra

journal homepage: www.elsevier.com/locate/jpaa

Bounding invariants of fat points using a coding theory construction

Ştefan O. Tohăneanu [a,*], Adam Van Tuyl [b]

[a] Department of Mathematics, The University of Western Ontario, London, ON N6A 5B7, Canada

[b] Department of Mathematical Sciences, Lakehead University, Thunder Bay, ON P7B 5E1, Canada

ARTICLE INFO

Article history:
Received 10 November 2011
Received in revised form 20 February 2012
Available online 29 June 2012
Communicated by A.V. Geramita

MSC:
Primary: 13D02
Secondary: 13D40; 94B27

ABSTRACT

Let $Z \subseteq \mathbb{P}^n$ be a fat point scheme, and let $d(Z)$ be the minimum distance of the linear code constructed from Z. We show that $d(Z)$ imposes constraints (i.e., upper bounds) on some specific shifts in the graded minimal free resolution of I_Z, the defining ideal of Z. We investigate this relation in the case that the support of Z is a complete intersection; when Z is reduced and a complete intersection we give lower bounds for $d(Z)$ that improve upon known bounds.

1. Introduction and Notations

Let $\mathbb{K}$ be a field of characteristic zero. Let $X = \{P_1, \ldots, P_s\} \subset \mathbb{P}^n$ be a reduced set of points not all contained in a hyperplane. A *fat point scheme* Z in $\mathbb{P}^n$ with *support* $\mathrm{Supp}(Z) = X$, and denoted

$$Z = m_1P_1 + \cdots + m_sP_s$$

is the zero-dimensional scheme defined by $I_Z = I_{P_1}^{m_1} \cap \cdots \cap I_{P_s}^{m_s} \subset R = \mathbb{K}[x_0, \ldots, x_n]$, where I_{P_i} is the defining ideal of the point P_i. The scheme Z is sometimes called a *set of fat points*. We call m_i the *multiplicity* of the point P_i. When all the m_i's are equal, we say Z is *homogeneous*.

To a fat point scheme we associate a linear code with generating matrix

$$A(Z) = [\ \underbrace{c_1 \ \cdots \ c_1}_{m_1} \ \ \cdots \ \ \underbrace{c_s \ \cdots \ c_s}_{m_s}\ ],$$

where each c_i is a column vector with entries equal to the homogeneous coordinates of the point P_i. This linear code has parameters $[m_1 + \cdots + m_s, n+1, d]$, where d denotes, as usual, the minimum Hamming distance of the code. Depending on the situation, d (denoted with $d(Z)$) will be called *the minimum distance of the matrix* $A(Z)$, or *the minimum distance of the fat point scheme* Z.

Note that in the matrix $A(Z)$, if we replace a column c_i with any of its (nonzero) scalar multiples, or if we permute in any way the columns of $A(Z)$, the parameters of this linear code do not change. As a consequence of this simple observation one can create a fat point scheme Z from any generating matrix of any linear code, by identifying the columns of this matrix with points (fat points, if some columns are proportional) in a projective space. Hansen [11], Gold et al. [7] and the first author [16] took this approach in the case when Z is reduced (i.e., $m_i = 1$, or the generating matrix has no proportional columns) to obtain bounds on the minimum distance using homological algebra. In particular, it was shown [7,15,16] that the minimum

* Corresponding author.
E-mail addresses: stohanea@uwo.ca (Ş.O. Tohăneanu), avantuyl@lakeheadu.ca (A. Van Tuyl).
URLs: http://www.math.uwo.ca/~stohanea/ (Ş.O. Tohăneanu), http://flash.lakeheadu.ca/~avantuyl/ (A. Van Tuyl).

0022-4049/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.jpaa.2012.06.004

distance d can be bounded below in terms of the graded shifts appearing in the graded minimal free resolution of R/I_Z. The lower bounds of $d = d(Z)$ can be interpreted as upper bounds for the corresponding homological invariants of Z; our main goal is to consider the same problem, but we drop the condition that Z is reduced.

Let $Z \subseteq \mathbb{P}^n$ be any zero-dimensional (arithmetically) Cohen–Macaulay subscheme. Let $R = \mathbb{K}[x_0, \ldots, x_n]$, and let $I = I_Z$ be the ideal of Z. Suppose that the graded minimal free resolution of R/I has the form

$$0 \to F_n = \bigoplus_{j=1}^{u_n} R(-a_{j,n}) \to \cdots \to F_1 = \bigoplus_{j=1}^{u_1} R(-a_{j,1}) \to R \to R/I \to 0.$$

We set $t_i = \min_j\{a_{j,i}\}$, for each $i = 1, \ldots, n$, and we call $s_n(Z) = t_n - n$ the *minimum socle degree* of Z.

Remark 1.1. We are abusing terminology slightly in the above definition. Since R/I is a Cohen–Macaulay ring of dimension 1, we can find a linear form L that is a nonzero divisor on R/I. Then, the ring $A = R/(I, L)$ is an Artinian ring. The socle of this ring is $\mathrm{soc}(A) = 0 : \overline{m}$ where $\overline{m} = \bigoplus_{j\geq 1} A_j$. The socle is an ideal of A; it can be shown that the degrees of the minimal generators of this ideal are encoded into the graded shifts at the end of the graded minimal resolution of R/I, but shifted by n (see [12] for more details). We call $s_n(Z)$ the minimum socle degree to recognize this connection.

When Z is reduced, the homological lower bounds for the minimum distance mentioned above are expressed in terms of the minimum socle degree, that is,

$$d(Z) \geq s_n(Z).$$

One can observe that the minimum distance puts constraints on the shifts in the graded minimal free resolution of Z: $d(Z) + n \geq t_n \geq t_{n-1} + 1 \geq \cdots \geq t_1 + n - 1$. Example 4.1 shows that the minimum distance will never precisely determine the minimum socle degree. Nevertheless, in [16] it is shown that $d(Z) = s_n(Z)$ is attained for a family of examples due to J. Migliore.

The goal of this paper is to obtain similar constraints for the graded minimal free resolution of a fat point scheme. Once we add multiplicities to the points, even when the support is as nice as possible (e.g., complete intersection), the shifts in the resolution change with no visible pattern.

In this paper, we take the point-of-view of describing how $d(Z)$, the minimum distance of a linear code constructed from Z, can be used to bound homological invariants of I_Z. One could invert this point-of-view by studying how homological invariants are related to the minimum distance, and linear codes in general. The references [7,11,15] took this second approach. Because some of our results do not require $char(\mathbb{K}) = 0$, these results could also be used to study linear codes. We see our results as complementing ongoing research to algebraically study linear codes. For example, the references [3,17] provide an entry point for readers who would like to learn more about coding theory from an algebraic geometric perspective. Feng et al. [4] present a version of Bézout's Theorem using resultants to address a lower bound for the minimum distance of a special class of algebraic geometric codes. And more recently, Sarmiento et al. [14] used algebraic methods to study problems arising from coding theory.

Our paper is structured as follows. In Section 2.1 we present a short introduction to the study of the minimum distance of a linear code. We consider the relationship between the minimum distance of the linear code created from a fat point scheme Z and the minimum distance of the linear code constructed from $X = \mathrm{Supp}(Z)$ (Theorem 2.4). The bounds obtained are optimal, as shown by examples. Since we have not found this result in the literature, we decided to write down the detailed proof, even though the result seems to be natural. In Section 2.2, Theorem 2.8 finds an upper bound for the first homological invariant of the fat point scheme Z in terms of the minimum distance of the associated linear code. The invariant considered is t_1, the minimal degree of a generator of I_Z. In Section 3 we present our main result, Theorem 3.7, which gives an upper bound for the minimum socle degree of the fat point scheme in terms of the minimum distance of its support. The main tool used is the machinery of separators of fat points developed in [10]. In Section 4, we specialize to the case that the support of the fat points Z in $\mathbb{P}^n$ is a complete intersection. In particular, we use Bézout's Theorem in Corollary 4.8 to give new lower bound on $d(Z)$.

2. Minimal degree of hypersurfaces containing Z

2.1. The minimum distance of a linear code

Let $\mathbb{K}$ be any field, and let $n \geq 1$ and $s \geq n + 1$ be two integers. A *linear code* $\mathcal{C}$ of length s and dimension $n + 1$ is the image of an injective $\mathbb{K}$-linear map $\phi : \mathbb{K}^{n+1} \to \mathbb{K}^s$. The *minimum (Hamming) distance* d of $\mathcal{C}$ is the minimum number of nonzero entries in a nonzero element (codeword) in $\mathcal{C}$. The numbers s, $n + 1$ and d are called *the parameters* of $\mathcal{C}$, and the code is called an $[s, n + 1, d]$-code.

Any matrix representation of ϕ is called a *generating matrix*. This representation is an $(n + 1) \times s$ matrix with entries in $\mathbb{K}$, of rank $n + 1$. Usually one writes this matrix representation of ϕ in the standard bases of $\mathbb{K}^{n+1}$ and $\mathbb{K}^s$. We can reverse the process: if A is an $(n + 1) \times s$ matrix of rank $n + 1$, we can create a linear code having A as a generating matrix, by constructing the map ϕ from A, using the standard bases.

Let $c_1, \ldots, c_s \in \mathbb{K}^{n+1}$ be $s \geq n+1$ vectors which have the property that no vector is a scalar multiple of another vector. That is, for every $i \neq j$, $c_i \neq ec_j$ for every $0 \neq e \in \mathbb{K}$. Let

$$A(X) = \begin{bmatrix} c_1 & \cdots & c_s \end{bmatrix},$$

and assume that the vectors c_i have been picked so that $\operatorname{rank}(A(X)) = n+1$. We call this matrix *reduced*. With the same vectors, fix integers $m_1, \ldots, m_s$, and set

$$A(Z) = \begin{bmatrix} \underbrace{c_1 \ \cdots \ c_1}_{m_1} & \cdots & \underbrace{c_s \ \cdots \ c_s}_{m_s} \end{bmatrix}. \tag{2.1}$$

When $m_1 = \cdots = m_s = 1$, then $A(Z) = A(X)$. If $m_i > 1$, then we say $A(Z)$ is *non-reduced*, and we call $A(X)$ the *reduced matrix* associated to $A(Z)$.

Definition 2.1. If A is an $(n+1) \times s$ matrix with entries in a field $\mathbb{K}$ with rank $n+1$, then the *minimum distance of A* is

$$d(A) = \min\{d \mid \text{there exists } s-d \text{ columns of } A \text{ that span an } n\text{-dimensional space}\}.$$

If $A = A(X)$, respectively, $A = A(Z)$, we will denote $d(A)$ by $d(X)$, respectively $d(Z)$.

Remark 2.2. If $\mathcal{C} \subseteq \mathbb{K}^s$ is a linear code with parameters $[s, n+1, d]$, then d is equal to the minimum distance of any generating matrix of $\mathcal{C}$, as we defined above.

We give a simple linear algebra argument for this fact. Suppose that

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,s} \\ \vdots & \vdots & & \vdots \\ a_{n+1,1} & a_{n+1,2} & \cdots & a_{n+1,s} \end{bmatrix}$$

is a generating matrix for $\mathcal{C}$. Denote with $r_1, \ldots, r_{n+1}$ the rows of A, and with $c_1, \ldots, c_s$ the columns. It is enough to show that there exists a codeword v (so a linear combination of the r_i's) with j zero entries in positions $i_1, \ldots, i_j$ if and only if the dimension of the vector space spanned by $c_{i_1}, \ldots, c_{i_j}$ is $\leq n$.

($\Rightarrow$) Let $v = u_1r_1 + \cdots + u_{n+1}r_{n+1}$, $u_i \in \mathbb{K}$ be a codeword with the first j entries equal to zero. This means that

$$u_1a_{1,1} + \cdots + u_{n+1}a_{n+1,1} = 0, \ \ldots, \ u_1a_{1,j} + \cdots + u_{n+1}a_{n+1,j} = 0.$$

Equivalently,

$$c_1, \ldots, c_j \in \{(x_1, \ldots, x_{n+1}) \in \mathbb{K}^{n+1} \mid u_1x_1 + \cdots + u_{n+1}x_{n+1} = 0\}.$$

So we have j points of $\mathbb{K}^{n+1}$ on a hyperplane, which implies

$$\dim \operatorname{span}\langle c_1, \ldots, c_j\rangle \leq n.$$

($\Leftarrow$) Suppose $\dim \operatorname{span}\langle c_1, \ldots, c_j\rangle \leq n$. If we consider the matrix whose ith row is given by c_i, i.e., take the transpose of the matrix with columns given by c_i's, then this matrix has rank at most n. But this means that the homogeneous system of equations in the variables $y_1, \ldots, y_{n+1}$

$$\begin{aligned} a_{1,1}y_1 + \cdots + a_{n+1,1}y_{n+1} &= 0 \\ &\vdots \\ a_{1,j}y_1 + \cdots + a_{n+1,j}y_{n+1} &= 0 \end{aligned}$$

must have a nontrivial solution $(u_1, \ldots, u_{n+1})$. This now means that the codeword $v = u_1r_1 + \cdots + u_{n+1}r_{n+1}$ has the first j entries equal to zero.

Remark 2.3. Suppose we are given any $t \geq n+1$ vectors in $a_1, \ldots, a_t \in \mathbb{K}^{n+1}$, such that $A = \begin{bmatrix} a_1 & \cdots & a_t \end{bmatrix}$ has rank $n+1$. Then, rescaling any proportional vectors or permuting columns of A does not change the value of the minimum distance $d(A)$ for this matrix.

The value of $d(Z)$ is related to $d(X)$ as follows:

Theorem 2.4. *Let $A(Z)$ be a matrix of the form (2.1) and assume that the columns of $A(Z)$ have also been permuted so that $m_1 \geq m_2 \geq \cdots \geq m_s$. If $A(X)$ is the reduced matrix associated to $A(Z)$, and $d(X) = d$, then*

$$m_1 + \cdots + m_d \geq d(Z) \geq m_{s-d+1} + \cdots + m_s.$$

In addition, if $m_1 = \cdots = m_s = m$, then $d(Z) = md(X)$.

Proof. Let

$$\Lambda = \left\{W = \{c_{i_1}, \ldots, c_{i_e}\} \subseteq \{c_1, \ldots, c_s\} \mid \dim(\mathrm{span}\langle W\rangle) = n\right\},$$

i.e., Λ is the collection of all e columns that span an n-dimensional space. In particular, since $d(X) = d$, we can find $s - d$ columns $c_{i_1}, \ldots, c_{i_{s-d}}$ such that $\{c_{i_1}, \ldots, c_{i_{s-d}}\} \in \Lambda$. So, if $W \in \Lambda$, then $n \leq |W| \leq s - d$, where the first inequality comes from the fact that one needs at least n vectors to span an n-dimensional space.

Computing $d(Z)$ is equivalent to finding the maximum number of column vectors of $A(Z)$ that span an n-dimensional space. If any column of $A(Z)$ is used to span this n-dimensional space, we should also take all copies of that column; each extra column does not contribute to the dimension (being a scalar multiple of the first column) but it contributes to the total number of columns being used.

Thus, if $M = m_1 + \cdots + m_s$, we can find e distinct columns $c_{i_1}, \ldots, c_{i_e}$ such that the following $M - d(Z)$ columns of $A(Z)$

$$\{\underbrace{c_{i_1}, \ldots, c_{i_1}}_{m_{i_1}}, \ldots, \underbrace{c_{i_e}, \ldots, c_{i_e}}_{m_{i_e}}\}$$

span an n-dimensional subspace of $\mathbb{K}^{n+1}$. But then $\{c_{i_1}, \ldots, c_{i_e}\} \in \Lambda$. Thus

$$M - d(Z) = \max\{m_{i_1} + \cdots + m_{i_e} \mid \{c_{i_1}, \ldots, c_{i_e}\} \in \Lambda\}.$$

So $M - d(Z) \geq m_{i_1} + \cdots + m_{i_e}$ for all $W = \{c_{i_1}, \ldots, c_{i_e}\} \in \Lambda$. Because there must exist $W \in \Lambda$ with $|W| = s - d$, we obtain that

$$M - d(Z) \geq m_{i_1} + \cdots + m_{i_{s-d}},$$

for some $i_1, \ldots, i_{s-d} \in [s]$.

If one has a (finite) decreasing (not necessarily strictly) sequence of numbers, then the sum of any k terms of this sequence is greater than or equal to the sum of the last k terms of the sequence. In our case the sequence is $m_1 \geq m_2 \geq \cdots \geq m_s$, and $k = s - d$. So

$$M - d(Z) \geq m_{d+1} + \cdots + m_s,$$

and therefore

$$m_1 + \cdots + m_d \geq d(Z).$$

Alternatively, we can write

$$d(Z) = \min\left\{ m_{j_1} + \cdots + m_{j_{s-e}} \;\middle|\; \begin{array}{c} \{j_1, \ldots, j_{s-e}\} = [s] \setminus \{i_1, \ldots, i_e\} \\ \text{with } \{c_{i_1}, \ldots, c_{i_e}\} \in \Lambda \end{array} \right\}.$$

Because any $W \in \Lambda$ has $|W| \leq s - d$, the smallest sum we can have contains $s - (s - d) = d$ terms. Moreover, since $m_1 \geq m_2 \geq \cdots \geq m_s$, we must have

$$d(Z) \geq m_{s-d+1} + \cdots + m_s.$$

When $m_1 = \cdots = m_s = m$, our two bounds give $md \geq d(Z) \geq md$. □

Remark 2.5. When $m_1 = \cdots = m_s = m$, then the corresponding linear code is sometimes called a *m-fold repetition code* (see [18]).

Example 2.6. Both of the bounds of Theorem 2.4 can be attained. Consider the following two matrices with entries in $\mathbb{F}_2$, the finite field with two elements:

$$A(Z_1) = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \quad \text{and} \quad A(Z_2) = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

These two matrices have the same reduced associated matrix

$$A(X) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix},$$

which has $d = d(X) = 1$.

For $A(Z_1)$ we have $d(Z_1) = 3$, and $m_1 = 3$, $m_2 = m_3 = m_4 = 2$. So the upper bound in Theorem 2.4 is attained. For $A(Z_2)$, we have $d(Z_2) = 1$, and $m_1 = 2$, $m_2 = m_3 = m_4 = 1$. In this case, the lower bound in Theorem 2.4 is attained.

2.2. An upper bound for t_1

Let $\mathbb{K}$ be any field and let $Z \subset \mathbb{P}^n_{\mathbb{K}}$ be a fat point scheme defined by $I_Z \subset R = \mathbb{K}[x_0, \dots, x_n]$. Let X be the support of Z, so X is a reduced finite set of points. Assume that they are not all contained in a hyperplane in $\mathbb{P}^n$.

As described above, let $A(X)$ be the reduced matrix associated to X and let $A(Z)$ the non-reduced matrix associated to Z. Let $d(X)$, and $d(Z)$ respectively, be the minimum distances of these matrices.

Remark 2.7. We can reinterpret $d(X)$ as a geometric condition. Let $hyp(X)$ denote the maximum number of points of X contained in a hyperplane. Then

$$d(X) = |X| - hyp(X).$$

We can observe this by noting that the columns corresponding to the points in the hyperplane must span a vector space of dimension n.

The ring R/I_Z has a graded minimal free resolution as given in the introduction. Let $\alpha(I_Z) := t_1 = \min\{u \mid (I_Z)_u \neq 0\}$. So $\alpha(I_Z)$ is the minimal degree of a hypersurface containing Z.

Theorem 2.8. *Let $Z = m_1P_1 + \cdots + m_sP_s \subseteq \mathbb{P}^n$ be a fat point scheme. Set $m(Z) = \max\{m_1, \dots, m_s\}$. Then*

$$d(Z) \geq \alpha(I_Z) - m(Z).$$

Proof. We first consider the case that $A(Z) = A(X)$, i.e., $m_i = 1$ for $i = 1, \dots, s$ for any integer $s \geq n + 1$. Suppose that $d(X) < \alpha(I_X) - 1$. Because X does not lie in a hyperplane, $\alpha(I_X) \geq 2$. From Remark 2.7, there is a hyperplane of equation $H = 0$ that contains $s - d(X)$ of the points of X. For the remaining $d(X)$ points, say $Q_1, \dots, Q_{d(X)}$, let L_i be any linear form in the ideal of the point Q_i. Then the hypersurface defined by $G = H \cdot L_1 \cdots L_{d(X)}$ passes through all the points of X, and $\deg G = 1 + d(X) < \alpha(I_X)$, a contradiction. So $d(X) \geq \alpha(I_X) - 1$.

We now proceed by induction on the tuple $(s, (m_1, \dots, m_s))$, that is, we assume that the statement holds for all tuples of the form $(s, (a_1, \dots, a_s))$ with

$$(\underbrace{1, \dots, 1}_{s}) \preceq (a_1, \dots, a_s) \prec (m_1, \dots, m_s),$$

or for all tuples of the form $(s - 1, (a_1, \dots, \hat{a}_i, \dots, a_s))$ where $s - 1 \geq n + 1$ and

$$(\underbrace{1, \dots, 1}_{s-1}) \preceq (a_1, \dots, \hat{a}_i, \dots, a_s) \prec (m_1, \dots, \hat{m}_i, \dots, m_s).$$

Here $\hat{}$ denotes the removal of an element from a tuple, and $(a_1, \dots, a_n) \preceq (b_1, \dots, b_n)$ if and only if $a_i \leq b_i$ for all i.

Let

$$A(Z) = \left[\ \underbrace{c_1 \ \cdots \ c_1}_{m_1} \quad \cdots \quad \underbrace{c_s \ \cdots \ c_s}_{m_s}\ \right].$$

Denote $d(Z) = d$ and $A(Z) = A$. From the definition, we can find d columns such that $M - d$ is the maximum number of columns in A that span an n-dimensional vector space. Here, $M = m_1 + \cdots + m_s$. Let Ω denote the set of these $M - d$ columns.

Let c be any column of A, with $c \notin \Omega$. Such a column exists, because if every column of A belonged to Ω, then the rank of A would not be $n + 1$.

Let A' be the matrix obtained from A after removing the column c. We now consider two cases.

Case 1. $\mathrm{rank}(A') = n + 1$.

Because $c \notin \Omega$, then Ω consists of columns of A', and the columns in Ω span an n-dimensional vector space. If we let d' denote the minimum distance of A', we then have $|\Omega| \leq (M - 1) - d'$. But because $|\Omega| = M - d$, we obtain $d \geq d' + 1$.

After permuting the columns of A, we can assume that we have removed the first column of A to construct A'. We then associate to A' the fat point scheme $Z' = (m_1 - 1)P_1 + m_2P_2 + \cdots + m_sP_s$.

Let $F \in (I_{Z'})_{\alpha(I_{Z'})}$ be any form of smallest degree in $I_{Z'}$, and let $L \in (I_{P_1})_1$ be any linear form in the ideal I_{P_1}. Then $FL \in (I_Z)_{\alpha(I_{Z'})+1}$, whence

$$\alpha(I_{Z'}) + 1 \geq \alpha(I_Z).$$

If $m_1 \geq 2$, then by induction we have that $d' = d(Z') \geq \alpha(Z') - m(Z')$. Similarly, if $m_1 = 1$, then we must have $s - 1 \geq n + 1$. This is because if we remove the first column from A, the columns of A' all correspond to points in the set $\{P_2, \dots, P_s\}$. Since the matrix A' has rank $n + 1$, we must have at least $n + 1$ distinct points in this set. But then by induction, we also know that $d' = d(Z') \geq \alpha(Z') - m(Z')$.

Because $m(Z) \geq m(Z')$, when we put together our pieces, we find the desired bound:

$$d(Z) \geq d(Z') + 1 \geq \alpha(I_{Z'}) - m(Z') + 1 \geq \alpha(I_Z) - m(Z).$$

Case 2. $\mathrm{rank}(A') = n$.

If $\mathrm{rank}(A') = n$, then the column c only appears in A exactly once. Furthermore, all the $M-1$ columns of A' span an n-dimensional vector space, and therefore

$$M - 1 \leq M - d,$$

and so $d = 1$, because the minimum distance must be positive.

After permuting the columns of A, we can assume that c is the first column c_1. Moreover, the distinct columns $c_2, \ldots, c_s$ in A span an n-dimensional vector space. This means that the points associated to these columns are contained in a hyperplane defined by a linear form H. So

$$H^{m(Z)} \in I_2^{m_2} \cap \cdots \cap I_s^{m_s}.$$

Let $L \in I_1$ be a linear form vanishing at the point associated to c_1. Then $L \cdot H^{m(Z)} \in I_Z$, and therefore $m(Z) + 1 \geq \alpha(I_Z)$ which gives us

$$d = 1 \geq \alpha(I_Z) - m(Z)$$

for this case as well. $\square$

When $Z = X$ is reduced, the bound we obtained in the previous theorem can only be attained in a very special situation.

Theorem 2.9. *Let $X = \{P_1, \ldots, P_s\}$ be a reduced set of points, not all contained in a hyperplane. Then $d(X) = \alpha(I_X) - 1$ if and only if $s-1$ points of X lie on a hyperplane.*

Proof. ($\Leftarrow$) The above theorem gives $d(X) \geq \alpha(I_X) - 1$. On the other hand, the set of points X do not lie on a hyperplane, so $\alpha(I_X) \geq 2$. In addition, if $s-1$ points of X lie on a hyperplane, this implies that the minimum distance of $A(X)$ is 1 since the $s-1$ columns corresponding to the points on the hyperplane span an n-dimensional vector space. So, $1 = d(X) \geq \alpha(I_X) - 1 \geq 2 - 1$, which gives the desired conclusion.

($\Rightarrow$) Suppose that $s' < s - 1$ is the maximum number of points of X that lie on a hyperplane. Let H be the linear form defining this hyperplane. By definition, $s - d(X) = s'$. Pick any two points of X not in this hyperplane, and let L be any linear form that vanishes at these two points. For any of the remaining $t = s - (s'+2) \geq 0$ points, let L_i be any linear form vanishing at that point. Then $G = H \cdot L \cdot L_1 \cdots L_t$ is a form in the ideal of the points of X. Furthermore

$$\deg G = t + 2 = s - s' = s - (s - d(X)) = d(X) = \alpha(I_X) - 1.$$

We have a contradiction since $(I_X)_i = (0)$ for all $i < \alpha(I_X)$. $\square$

Example 2.10. When Z is not reduced, one can attain the bound in Theorem 2.8 as well. Let $P_1 = [0:1:0]$, $P_2 = [1:0:0]$, $P_3 = [1:1:0]$, $P_4 = [0:0:1]$ be four points in $\mathbb{P}^2$. Consider $Z = 2P_1 + 2P_2 + P_3 + P_4$. We have $\alpha(I_Z) = 3$ and $m(Z) = 2$.

We have

$$A(Z) = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

which has $d(Z) = 1$.

Example 2.11. Since there are no restrictions on the base field $\mathbb{K}$, the statement in Theorem 2.8 can have applications in coding theory; it gives a lower bound for the minimum distance of $A(Z)$. This lower bound does not depend on $d(X)$, where $X = \mathrm{Supp}(Z)$, as Theorem 2.4 does.

Furthermore, the lower bound of Theorem 2.8 improves the bound of Theorem 2.4 in certain cases. For example, let $X = \{P_1, \ldots, P_6\}$ be six points in $\mathbb{P}^2$ where P_4, P_5, P_6 all lie on a line, and none of P_1, P_2, or P_3 lie on this line, and moreover, there is no line that passes through these three points. By our choice of points, $hyp(X) = 3$, and thus $d(X) = 6 - 3 = 3$.

Now consider the fat point scheme $Z = 5P_1 + 5P_2 + 5P_3 + P_4 + P_5 + P_6$. We have $m_1 = m_2 = m_3 = m(Z) = 5$, and $m_4 = m_5 = m_6 = 1$. Theorem 2.4 gives the lower bound $d(Z) \geq m_4 + m_5 + m_6 = 3$. However, for this set of fat points, $\alpha(I_Z) = 9$, whence by Theorem 2.8 we have $d(Z) \geq \alpha(I_Z) - m(Z) = 9 - 5 = 4$. So, the lower bound of Theorem 2.8 is better in this case.

3. The minimum socle degree of a homogeneous fat point scheme

Let $\mathbb{K}$ be a field of characteristic zero. Let $Z = mP_1 + \cdots + mP_s \subset \mathbb{P}^n$ be a homogeneous fat point scheme with $X = \mathrm{Supp}(Z) = \{P_1, \ldots, P_s\}$ not contained in a hyperplane. With the notations above, in this section we prove one of the main results of the paper:

$$s_n(Z) \le md(X).$$

(Note that we assume $\mathbb{K}$ has characteristic zero so that we can make use of a result found in [10] on separators of fat points. In particular, the result that we require from [10] is based upon a mapping cone construction of a graded minimal free resolution of I_Z; the maps that appear in this construction may change if we consider a field of characteristic $p > 0$. A careful analysis of [10] would be required to determine if the results of this section still hold in nonzero characteristics.)

Before we prove this result, we will make some remarks on the results obtained in the previous section for the case of homogeneous fat points. First, as observed in Theorem 2.4, $d(Z) = md(X)$. Second, the result in Theorem 2.8 is immediate in this case: if $f \in I_X$ is of degree $\alpha(I_X)$, then $f^m \in I_Z$, and hence $m\alpha(I_X) \ge \alpha(I_Z)$. With $d(Z) = md(X)$ and $d(X) \ge \alpha(I_X) - 1$, we indeed obtain that $d(Z) \ge \alpha(I_Z) - m$.

An interesting question remains: When is this bound attained? A simple computation shows that the bound is attained whenever $d(X) = 1$ and $\alpha(I_Z) = m\alpha(I_X)$. Now, looking at Example 2.10, with $Z = mP_1 + mP_2 + mP_3 + mP_4$, when $m = 2$ we have $\alpha(I_Z) = 4 = 2\alpha(I_X)$, whereas when $m \ge 3$, $\alpha(I_Z) \le 2m - 1$.

In general there is no control on $\alpha(I_Z)$ as we vary m. As we can see in the second part of the example below, some "random" behavior happens in general for $s_n(Z)$ when Z is a homogeneous fat point scheme.

Example 3.1. Let $X = \{P_1, P_2, P_3, P_4, P_5\} \subseteq \mathbb{P}^2$ where $P_1 = [1 : 0 : 0], P_2 = [0 : 1 : 0], P_3 = [0 : 0 : 1], P_4 = [1 : 1 : 0]$, and $P_5 = [1 : 3 : 1]$. Set $Z = mP_1 + mP_2 + mP_3 + mP_4 + mP_5$, with $m \ge 1$. We have that $d(X) = 2 \ge 2 = \alpha(I_X)$, and $d(Z) = md(X) = 2m$. For $m = 1, \ldots, 7$, we calculate the minimum socle degree of I_Z:

m	1	2	3	4	5	6	7
$s_2(Z)$	2	4	6	8	10	12	14

Let $X = \{P_1, P_2, P_3, P_4\} \subseteq \mathbb{P}^2$ where $P_1 = [1 : 0 : 0], P_2 = [0 : 1 : 0], P_3 = [0 : 0 : 1]$, and $P_4 = [1 : 1 : 0]$, and set $Z = mP_1 + mP_2 + mP_3 + mP_4$ with $m \ge 1$. We have $d(X) = 1 = 2 - 1 = \alpha(I_X) - 1$ and $d(Z) = md(X) = m$. For $m = 1, \ldots, 7$, we calculate $s_2(Z)$:

m	1	2	3	4	5	6	7
$s_2(Z)$	1	3	5	6	8	10	11

Before we state and prove Theorem 3.7, we shall need the notion of a separator of a fat point, as found in [10].

Definition 3.2. Let $Z = m_1P_1 + \cdots + m_sP_s \subseteq \mathbb{P}^n$ be a set of fat points, and suppose that $Z' = m_1P_1 + \cdots + (m_i - 1)P_i + \cdots + m_sP_s$ for some $i = 1, \ldots, s$. (If $m_i = 1$, we simply omit the point P_i in Z'.) We call $F \in R = \mathbb{K}[x_0, \ldots, x_n]$ a *separator of P_i of multiplicity m_i* if $F \in I_{Z'} \setminus I_Z$.

When all of the m_is equal one in the above definition, we recover the definition of a separator of a reduced point as found in [1,2,6]. We now apply [10, Theorem 5.4].

Theorem 3.3. *Let $Z = m_1P_1 + \cdots + m_sP_s \subseteq \mathbb{P}^n$ be a set of fat points, and suppose that $Z' = m_1P_1 + \cdots + (m_i - 1)P_i + \cdots + m_sP_s$ for some $i = 1, \ldots, s$. Let F be any separator of P_i of multiplicity of m_i of smallest degree, i.e., if F' is any other separator of P_i of multiplicity m_i, then* $\deg F' \ge \deg F$. *Then*

$$\deg F \ge s_n(Z).$$

Proof. Note that [10, Theorem 5.4] actually proves something stronger: if $\overline{G}$ is any minimal generator of the R-module $I_{Z'}/I_Z$, then $\deg G + n$ appears as a shift in the last module in the graded minimal free resolution of I_Z. Because $\overline{F}$ will be a minimal generator of $I_{Z'}/I_Z$ of smallest degree, $\deg F + n$ will appear as a shift in the last module in the graded minimal free resolution, and thus $\deg F + n - n \ge s_n(Z)$. □

We need one other result. In Remark 2.7, $hyp(X)$ denotes the maximum number of points of a reduced set of points X contained in some hyperplane. To obtain the maximum number of points of X contained in some hypersurface of degree a, by [13], one should compute $hyp(v_a(X))$, where v_a is the Veronese embedding of degree a of $\mathbb{P}^n$ into $\mathbb{P}^{N_a}$, where $N_a = \binom{n+a}{a} - 1$. Let us denote

$$d(X)_a = |X| - hyp(v_a(X)).$$

Observe that $d(X)_1 = d(X)$.

Remark 3.4. As an aside, $d(X)_a$ is the minimum distance of the evaluation code $\mathcal{C}(X)_a$ (see [11,17] for more details). However, we will not need this interpretation.

The following lemma will then constitute a key tool needed to prove our main result:

Lemma 3.5 ([15, Proposition 2.1]). *Let $X = \{P_1, \ldots, P_s\} \subseteq \mathbb{P}^n$ be a set of distinct reduced points. If $d(X)_b \ge 2$ for some b, then for all $1 \le a \le b - 1$, we have $d(X)_a \ge d(X)_{a+1} + 1$ and therefore $d(X)_a \ge b - a + 2$.*

Remark 3.6. Here is an intuitive, geometrical proof of the above lemma. Suppose that $s - d(X)_a$ points of X lie on a hypersurface of degree a. Then we need to have at least $s - d(X)_a + 1$ points lying on a hypersurface of degree $a + 1$. Indeed, if you take the hypersurface $V(F)$ of degree a containing the $s - d(X)_a$ points, and any hyperplane $V(L)$ through one of the remaining points, then the hypersurface $V(F \cdot L)$ of degree $a + 1$ will contain $s - d(X)_a + 1$ points. So, $d(X)_{a+1} \leq s - (s - d(X)_a + 1)$, i.e., $d(X)_{a+1} + 1 \leq d(X)_a$.

We come to our main theorem.

Theorem 3.7. *Let $Z = mP_1 + \cdots + mP_s \subseteq \mathbb{P}^n$ be a homogeneous set of fat points with $X = \mathrm{Supp}(Z)$ not contained in a hyperplane.*

(i) *If $d(X) \geq \alpha(I_X)$, then $s_n(Z) \leq md(X)$.*
(ii) *Otherwise, if $d(X) = \alpha(I_X) - 1$, then $s_n(Z) \leq 2m - 1$.*

Proof. From Theorem 2.4, we have that $d(Z) = md(X)$.

For each $P_i \in X$, let

$$\delta_i = \min\{\deg F \mid F(Q) = 0 \text{ for each } Q \in X \setminus \{P_i\} \text{ but } F(P_i) \neq 0\}.$$

Let $\delta = \min_{i=1}^{s}\{\delta_i\}$ be the minimum degree. After relabeling, we may assume that $\delta = \delta_1$. Let $X' = X \setminus \{P_1\}$ and let $F \in I_{X'} \setminus I_X$ be a separator of degree δ.

Let $G \in (I_X)_{\alpha(I_X)}$. Then

$$F \cdot G^{m-1} \in I_W \setminus I_Z,$$

where $W = (m-1)P_1 + mP_2 + \cdots + mP_s$. In other words, $F \cdot G^{m-1}$ is separator of P_1 of multiplicity m. So

$$\delta + (m-1)\alpha(I_X) \geq \Delta(Z),$$

where $\Delta(Z)$ is the smallest degree of a separator of P_1 of multiplicity m. By Theorem 3.3, we then have

$$\delta + (m-1)\alpha(I_X) \geq \Delta(Z) \geq s_n(Z).$$

(i) If $d(X) \geq \alpha(I_X)$, then $\delta \geq 2$. Otherwise, if $\delta = 1$, then $s - 1$ points of X will lie in a hyperplane. But by Corollary 2.9, this can only happen if $d(X) = \alpha(I_X) - 1$.

Also, $d(X)_{\delta-1} \geq 2$. If $d(X)_{\delta-1} \leq 1$, then there is a hypersurface of degree $\delta - 1$ that contains either all the points of X, or all but one point of X. But this would contradict our choice of δ; it is the smallest degree of a form that passes through all the points of X except one. So, by Lemma 3.5 with $b = \delta - 1$ and $a = 1$, we have $d(X) \geq \delta$. With this fact, and since $d(X) \geq \alpha(I_X)$, we obtain

$$d(Z) = md(X) = d(X) + (m-1)d(X) \geq \delta + (m-1)\alpha(I_X) \geq \Delta(Z) \geq s_n(Z).$$

(ii) If $d(X) = \alpha(I_X) - 1$, then $s - 1$ points of X lie on a hyperplane by Corollary 2.9. As shown in the proof of this corollary, this also implies $d(X) = 1$. Let $V(H)$ be the hyperplane through the $s - 1$ points, and let L be a linear form that vanishes at the remaining point off the hyperplane (say P_1). Then

$$H^m \cdot L^{m-1} \in I_W \setminus I_Z$$

where $W = (m-1)P_1 + mP_2 + \cdots + mP_s$. Hence, $H^m \cdot L^{m-1}$ is a separator of P_1 of multiplicity m. Thus, by Theorem 3.3,

$$2m - 1 \geq s_n(Z). \quad \square$$

Remark 3.8. Looking at Example 3.1, observe that the first part of this example gives that for each $m = 1, \ldots, 7$ the lower bound of Theorem 3.7(i) is attained. The second part shows that for $m = 1, 2$ and 3 the lower bound of Theorem 3.7(ii) is also attained.

We end this section with a question based upon our results.

Question 3.9. *Can we generalize the lower bound of Theorem 3.7 to non-homogeneous fat points? Is it true that $d(Z) \geq s_n(Z) - m(Z) + 1$, where $m(Z)$ is the maximum multiplicity of a point in Z, for any Z? In other words, because $s_n(Z) \geq \alpha(I_Z) - 1$, can Theorem 2.8 be improved to $d(Z) \geq s_n(Z) - m(Z) + 1 \geq \alpha(I_Z) - m(Z)$?*

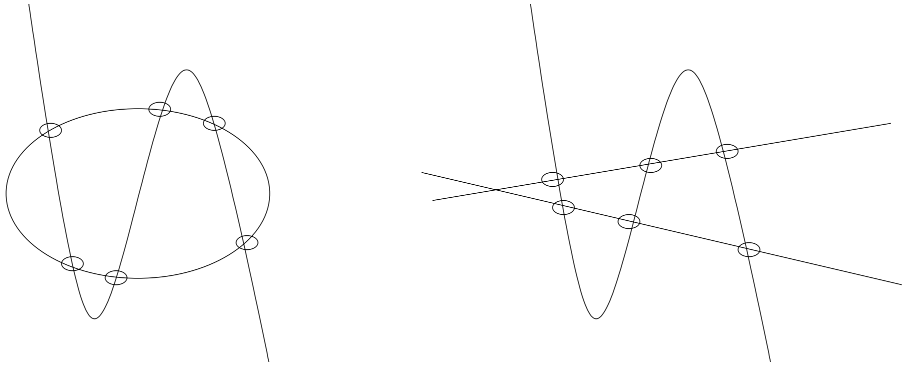
4. A case study: complete intersections

Reduced matrices of the form $A(X)$ were studied by Hansen [11] and Gold et al. [7]. In both cases, the authors focused on the case that the associated set of reduced points X was a complete intersection. (Their results were later generalized in [15] to the case that X was Gorenstein, and in [16] to the case that X was any reduced set of points.) Building upon their work, we consider matrices of the form $A(Z)$ when the support of the fat points Z is a complete intersection.

Recall that a set of points of $X \subseteq \mathbb{P}^n$ is a *complete intersection of type* $(d_1, \ldots, d_n)$ if there exists a regular sequence of homogeneous forms $F_1, \ldots, F_n \in R$ with $\deg F_i = d_i$ such that $I_X = (F_1, \ldots, F_n)$. We usually denote X by $CI(d_1, \ldots, d_n)$. Because the F_i's defining a complete intersection are homogeneous, any permutation of the F_i's is also a complete intersection. So, we can make the assumption that $d_1 \leq d_2 \leq \cdots \leq d_n$. Because we are interested in the case that $A(X)$ has full rank, we can also assume that $2 \leq d_1$. If $d_1 = 1$, then the set of points X would be contained in a hyperplane.

Recall that the theme of this paper is to study the shifts in the graded minimal free resolution in terms of the minimum distance of $A(Z)$. While some bounds can be found, the following example shows that this will not be enough.

Example 4.1. Consider the following two sets of points $X_1, X_2 \subseteq \mathbb{P}^2$, both examples of complete intersections of the form $CI(2, 3)$. In the first case the conic is irreducible, while in the second case the conic is reducible.



The graded minimal free resolutions of R/I_{X_1} and R/I_{X_2} are the same, i.e.,

$$0 \to R(-5) \to R(-2) \oplus R(-3) \to R \to R/I \to 0 \quad \text{with } I = I_{X_1} \text{ or } I_{X_2}.$$

We have $s_2(X_1) = s_2(X_2) = 5 - 2 = 3$. If A_1 and A_2 are the corresponding matrices (i.e., the columns of these matrices will be given by the homogeneous coordinates in the algebraic closure of $\mathbb{K}$ of the points), we see from Remark 2.7, that $d(A_1) = 6 - 2 = 4$, and $d(A_2) = 6 - 3 = 3$.

Indeed the bound in Theorem 3.7, with $m = 1$, is satisfied for both cases, that is, $d(A_i) \geq s_2(A_i)$ for $i = 1, 2$. But this example also shows that one cannot rely on the graded minimal free resolution alone to find the minimum distance.

4.1. Homogeneous fat points with complete intersection support

As shown in Theorem 3.7, we can bound $d(Z)$ in terms of $s_n(Z)$. In the case that $\mathrm{Supp}(Z)$ is a complete intersection, we can get an explicit value for $s_n(Z)$ when all the multiplicities are equal.

Lemma 4.2. *Let $Z = mP_1 + \cdots + mP_s \subseteq \mathbb{P}^n$ be a set of fat points with* $\mathrm{Supp}(Z) = CI(d_1, d_2, \ldots, d_n)$. *Then*

$$s_n(Z) = md_1 + d_2 + d_3 + \cdots + d_n - n.$$

Proof. The defining ideal of I_Z is I_X^m with $X = \mathrm{Supp}(Z)$. But I_X^m is a power of a complete intersection, so one can use the formula of [9, Theorem 2.1]. □

If we want to see for what such Z are the bounds in Theorem 3.7 attained, we obtain the following.

Theorem 4.3. *Let $X = CI(d_1, \ldots, d_n) \subseteq \mathbb{P}^n$ with $n \geq 2$, and let Z be the homogeneous set of fat points of multiplicity m whose support is X. Then*

$$md(X) = s_n(Z) \text{ if and only if } X = CI(2, 2).$$

Proof. First, we show that we can exclude the second part of Theorem 3.7 from consideration. Indeed, suppose that $d(X) = \alpha(I_X) - 1$. By the proof of Corollary 2.9, we must have $\alpha(I_X) = d_1 = 2$, and thus Theorem 4.2 implies that $s_n(Z) = 2m + d_2 + \cdots + d_n - n$. From Theorem 3.7, we have $s_n(Z) \leq 2m - 1$, and therefore, $d_2 + \cdots + d_n - n \leq -1$. But $2 = d_1 \leq d_2 \leq \cdots \leq d_n$ implies that $2(n-1) - n \leq d_2 + \cdots + d_n - n \leq -1$, thus giving us $n - 2 \leq -1$, that is, $n \leq 1$, thus giving the contradiction. Thus, we can assume that $d(X) \geq \alpha(I_X) = d_1$.

Suppose $s_n(Z) = md(X)$. From Theorem 3.7, $m = 1$, we have $d(X) \geq s_n(X) = d_1 + \cdots + d_n - n$ and, from Lemma 4.2, $s_n(Z) = md_1 + d_2 + \cdots + d_n - n$.

Denote $s_n(Z) = U$ and $ms_n(X) = V$. We then have $U = (m-1)d_1 + V/m$. Now we will have $U \geq V$ if and only if $(m-1)d_1 + V/m \geq V$. But this inequality is equivalent to

$$m(m-1)d_1 \geq (m-1)V.$$

So $md_1 \geq V$. But $V = ms_n(X)$, so $d_1 \geq s_n(X) = d_1 + d_2 + \cdots + d_n - n$. We thus get $U \geq V$ if and only if $n \geq d_2 + \cdots + d_n$. But $2 \leq d_2 \leq \cdots \leq d_n$, so we have $n \geq 2(n-1)$, i.e., $2 \geq n$. But this forces $n = 2$, $d_2 = 2$, and $d_1 = 2$.

Thus, unless $X = CI(2, 2)$, we have $ms_n(X) > s_n(Z)$, and therefore $md(X) \neq s_n(Z)$.

If $X = CI(2, 2)$, then $s_2(Z) = m \cdot 2 + 2 - 2 = 2m$. Since $d(X) = 2$ we have indeed that $s_2(X) = md(X)$. □

Lemma 4.2 also lets us recover a result of Gold et al. [7] as a corollary; their result is the case when all the multiplicities equal one.

Corollary 4.4. *Let $X = \{P_1, \ldots, P_s\} \subseteq \mathbb{P}^n$ be a reduced set of points. If $X = CI(d_1, \ldots, d_n)$, then*

$$d(X) \geq d_1 + d_2 + d_3 + \cdots + d_n - n.$$

Proof. By Theorem 3.7, $d(X) \geq s_n(X)$. Now use Theorem 4.2. □

4.2. Bézout's Theorem

It is known that the bound of Corollary 4.4 is far from optimal. For complete intersections of the form $X = CI(d_1, \ldots, d_n) \subseteq \mathbb{P}^n$, we will use Bézout's Theorem to improve known bounds.

There are many ways one can state Bézout's Theorem in $\mathbb{P}^n$. The version we shall use can be found in Chapter 6.2 of [5]. We thank the anonymous referee for pointing out that this version is valid also when $\mathbb{K}$ is an algebraically closed field of positive characteristic.

We first recall that the *degree* of a scheme $W \subseteq \mathbb{P}^n$, denoted by $\deg(W)$, is defined to be $(\dim W)!$ times the leading coefficient of the Hilbert polynomial of W.

Theorem 4.5 (*Bézout's Theorem*). *Let X be a projective subscheme of $\mathbb{P}^n$ with $\dim X \geq 1$. If $f \in \mathbb{K}[x_0, \ldots, x_n]$ is a homogeneous form such that no component of X is contained in $V(f)$, the variety defined by f, then*

$$\deg(X \cap V(f)) = \deg(f) \cdot \deg(X).$$

To make use of this theorem, we recall two standard facts:

- If W is a reduced finite set of points, then $\deg(W) = |W|$.
- If $W = CI(d_1, \ldots, d_r)$, then $\deg(W) = d_1 \cdots d_r$.

First, a general result:

Theorem 4.6. *Let Y be a curve in $\mathbb{P}^n$ with no component contained in a hyperplane. Let $V(f)$ be a hypersurface of degree $a > 1$ such that $X = Y \cap V(f)$ is a reduced zero-dimensional scheme. Then X has minimum distance*

$$d(X) \geq (a-1)\deg(Y).$$

Proof. Suppose that Y has a component W contained in $V(f)$. Then $W \subseteq X$. Since $\dim(X) = 0$, then $\dim(W) = 0$, and so $W = W_1 \cup \cdots \cup W_m$, where each W_i is set-theoretically a point in $\mathbb{P}^n$. Since a point is always contained in a hyperplane, we have contradicted our assumption that Y has no component in a hyperplane. So we can apply Bézout's Theorem to obtain

$$|X| = \deg(X) = a \cdot \deg(Y).$$

We have that $d(X) = |X| - hyp(X)$, so it suffices to show that $hyp(X) \leq \deg(Y)$. Suppose that $h = hyp(X) > \deg(Y)$ and that $V(L)$ is the hyperplane containing the h points of X. Since no component of Y is contained in $V(L)$, then $\dim(Y \cap V(L)) = 0$ and furthermore we can apply Bézout's Theorem once more to obtain that

$$\deg(Y \cap V(L)) = \deg(L) \cdot \deg(Y) = \deg(Y),$$

since $\deg(L) = 1$. Since $X \subset Y$, then $X \cap V(L) \subseteq Y \cap V(L)$. Therefore the h points of X lying on $V(L)$ should be contained in $Y \cap V(L)$. But then $\deg(Y \cap V(L)) \geq h$, which contradicts the assumption that $h > \deg(Y)$. □

Example 4.7. We can construct sets of points such that the bound in Theorem 4.6 is attained. Let $Y \subset \mathbb{P}^n$ be an irreducible curve, not contained in an hyperplane. Let g be a form of degree $a-1 \geq 1$ and let L be a linear form such that $X = V(L\cdot g) \cap Y$ is a reduced zero-dimensional scheme.

Since $V(L\cdot g) = V(L) \cup V(g)$, then $V(L) \cap Y \subseteq X$, is a reduced zero-dimensional scheme of degree $\deg(V(L) \cap Y) = \deg(Y)$. So the hyperplane $V(L)$ contains $\deg(Y)$ points of X. This implies that $hyp(X) \geq \deg(Y)$. But from Theorem 4.6 we have $hyp(X) \leq \deg(Y)$, and therefore we get an equality.

As a corollary, we improve the bound on $d(X)$ when X is complete intersection with an additional condition.

Corollary 4.8. *Let $X = CI(d_1, \ldots, d_n) \subseteq \mathbb{P}^n$, with $2 \leq d_1 \leq \cdots \leq d_n$. If $I_X = (F_1, \ldots, F_n)$, then for each $i = 1, \ldots, n$ let X_i be the complete intersection $CI(d_1, \ldots, \hat{d}_i, \ldots, d_n)$, with ideal $I_{X_i} = (F_1, \ldots, \hat{F}_i, \ldots, F_n)$. In addition, suppose that there exists an index $j \in \{1, \ldots, n\}$ such that X_j has no component contained in a hyperplane. Then*

$$d(X) \geq (d_1 - 1)d_2 d_3 \cdots d_n.$$

Proof. Because X is a reduced complete intersection, $|X| = d_1 \cdots d_n$. Also, for each i, X_i is a complete intersection curve of degree $\deg(X_i) = d_1 \cdots \hat{d}_i \cdots d_n$.

Let j be the index such that X_j has no component contained in a hyperplane. From Theorem 4.6, with $Y = X_j$, and $f = F_j$, we obtain

$$d(X) \geq (d_j - 1)d_1 \cdots \hat{d}_j \cdots d_n.$$

Since $d_1 \leq d_2 \leq \cdots \leq d_n$, then $d_2 \cdots d_n \geq d_1 \cdots \hat{d}_j \cdots d_n$. Hence, the assertion. $\square$

We expect that the hypothesis in Corollary 4.8 that there exists an X_j with no component contained in a hyperplane can be dropped. We make the following conjecture:

Conjecture 4.9. *Let $X = CI(d_1, \ldots, d_n) \subseteq \mathbb{P}^n$, with $2 \leq d_1 \leq \cdots \leq d_n$. Then $d(X) \geq (d_1 - 1)d_2d_3 \cdots d_n$.*

When $n = 2$, we only need Bézout's Theorem for curves to prove Conjecture 4.9.

Theorem 4.10. *Let $X = CI(d_1, d_2) \subseteq \mathbb{P}^2$, with $2 \leq d_1 \leq d_2$. Then $d(X) \geq (d_1 - 1)d_2$.*

Proof. Let $h = hyp(X)$, and suppose that $h > d_2$. Therefore, there is a line (since we are in $\mathbb{P}^2$) that contains $h > d_2$ points of X. Let L be the form that defines this line, and suppose that $I_X = (F_1, F_2)$. Bézout's Theorem for curves in $\mathbb{P}^2$ implies that $L|F_1$ since $V(L) \cap V(F_1)$ meet at $h > d_1$ points. Similarly, $L|F_2$ since $V(L) \cap V(F_2)$ meet at $h > d_2$ points. But then L divides $\gcd(F_1, F_2)$, contradicting the assumption that F_1 and F_2 form a regular sequence. $\square$

Remark 4.11. The bound of Theorem 4.10 improves the bound of Gold et al. [7] (see Corollary 4.4) when $3 \leq d_1$. Indeed, we have $d_1d_2 - d_2 > d_1 + d_2 - 2$ if and only if $d_1d_2 - d_1 = d_1(d_2 - 1) > 2(d_2 - 1) = 2d_2 - 2$ if and only if $d_1 \geq 3$. When $2 = d_1$, the two bounds are the same, i.e, $(d_1 - 1)d_2 = d_1 + d_2 - 2 = d_2$.

Acknowledgments

All the computations were done using *Macaulay 2* [8]. The second author was supported by a Discovery Grant from NSERC. We thank the anonymous referee for important comments and suggestions, especially for pointing out that the version of Bézout's Theorem that we use, also holds for algebraically closed fields of positive characteristic.

References

[1] S. Abrescia, L. Bazzotti, L. Marino, Conductor degree and socle degree, Matematiche (Catania) 56 (2001) 129–148.
[2] L. Bazzotti, Sets of points and their conductor, J. Algebra 283 (2005) 799–820.
[3] D. Cox, J. Little, D. O'Shea, Using Algebraic Geometry, in: GTM, vol. 185, Springer, 2005.
[4] G.-L. Feng, T.R.N. Rao, G. Berg, Generalized Bezout's theorem and its applications in coding theory, IEEE Trans. Inform. Theory 43 (1997) 1799–1810.
[5] A. Gathmann, Algebraic Geometry, University of Kaiserslautern 2002/2003, http://www.mathematik.uni-kl.de/~gathmann/alggeom.php.
[6] A.V. Geramita, P. Maroscia, L. Roberts, The Hilbert function of a reduced k-algebra, J. Lond. Math. Soc. 28 (1983) 443–452.
[7] L. Gold, J. Little, H. Schenck, Cayley–Bacharach and evaluation codes on complete intersections, J. Pure Appl. Algebra 196 (2005) 91–99.
[8] D.R. Grayson, M.E. Stillman, Macaulay 2, a software system for research in algebraic geometry, http://www.math.uiuc.edu/Macaulay2/.
[9] E. Guardo, A. Van Tuyl, Powers of complete intersections: graded Betti numbers and applications, Illinois J. Math 49 (2005) 265–279.
[10] E. Guardo, L. Marino, A. Van Tuyl, Separators of fat points in $\mathbb{P}^n$, J. Algebra 324 (2010) 1492–1512.
[11] J. Hansen, Linkage and codes on complete intersections, Appl. Algebra Engng Comm. Comput. 14 (2003) 175–185.
[12] A. Kustin, B. Ulrich, If the socle fits, J. Algebra 147 (1992) 63–80.
[13] J. Migliore, C. Peterson, A symbolic test for (i, j)-uniformity in reduced zero-dimensional schemes, J. Symbolic Comput. 37 (2004) 403–413.
[14] E. Sarmiento, M. Vaz Pinto, R.H. Villarreal, The minimum distance of parametrized codes on projective tori, Appl. Algebra Engng Comm. Comput. 22 (2011) 249–264.
[15] Ş. Tohăneanu, Lower bounds on minimal distance of evaluation codes, Appl. Algebra Engng Comm. Comput. 20 (2009) 351–360.
[16] Ş. Tohăneanu, The minimum distance of sets of points and the minimum socle degree, J. Pure Appl. Algebra 215 (2011) 2645–2651.
[17] M. Tsfasman, S. Vladut, D. Nogin, Algebraic Geometric Codes: Basic Notions, AMS, USA, 2007.
[18] E. Weiss, Linear codes of constant weight, SIAM J. Appl. Math. 14 (1966) 106–111.