ERROR-CORRECTION OF LINEAR CODES VIA COLON IDEALS

BENJAMIN ANZIS AND ŞTEFAN O. TOHÂNEANU

ABSTRACT. In this paper we show that errors in transmitted data can be thought of as codewords of minimum weight of new linear codes. To determine the errors we can then use methods specific to finding such special codewords. One of these methods consists of finding the primary decomposition of the saturation of a certain homogeneous ideal. When good messages (i.e., vectors with a unique nearest neighbor) are error-corrected, the saturated ideal is just the prime ideal of a point (so the primary decomposition is superfluously determined); the computation of this ideal can also be done by colon the original homogeneous ideal with a power of a certain variable. We then prove an upper bound for this power for MDS codes. Finally, we use the upper bound to describe the minimal graded free resolution of a certain class of ideals generated by products of linear forms.

1. INTRODUCTION

Let \( C \) be an \([n, k, d]\)–linear code with generating matrix (in canonical bases)

\[
G = \begin{pmatrix}
  a_{11} & a_{12} & \cdots & a_{1n} \\
  a_{21} & a_{22} & \cdots & a_{2n} \\
  \vdots & \vdots & & \vdots \\
  a_{k1} & a_{k2} & \cdots & a_{kn}
\end{pmatrix},
\]

where \( a_{ij} \in K \), any field.

By this, one understands that \( C \) is the image of the injective linear map

\[
\phi : K^k \xrightarrow{G} K^n.
\]

2010 Mathematics Subject Classification. Primary: 14G50; Secondary: 13D02, 94B35, 13D40, 11T71.

Keywords and phrases. linear codes, minimum distance, saturation, colon ideals, MDS codes, Castelnuovo-Mumford regularity, free resolutions.

The second author is the corresponding author.

Authors’ addresses: Department of Mathematics, University of Idaho, Moscow, ID 83844, anzi4123@vandals.uidaho.edu, tohaneanu@uidaho.edu.
\( n \) is the length of \( C \), \( k \) is the dimension of \( C \) and \( d \) is the minimum distance (or Hamming distance), the smallest number of non-zero entries in a non-zero codeword (i.e., element of \( C \)). For background on linear codes we recommend [11].

Also, for any vector \( w \in \mathbb{K}^n \), the weight of \( w \), denoted \( wt(w) \), is the number of non-zero entries in \( w \).

The most commonly used method for decoding a received message \( w \in \mathbb{K}^n \) is to find the codeword \( v \in C \) which minimizes \( wt(w - v) \) (i.e. \( v \) is the nearest neighbor of \( w \)), and decode \( w \) to \( \phi^{-1}(v) \). Of course, a \( w \notin C \) might have more than one nearest neighbor. In this case the nearest neighbor algorithm fails. Fortunately, under certain conditions (see Proposition 2.1 in [4, Chapter 9]), error detection and correction are guaranteed to succeed:

- any \( d - 1 \) errors in a received vector can be detected, meaning that if there is a \( v \in C \) with \( 0 < wt(w - v) \leq d - 1 \), then \( w \notin C \), and
- if \( d \geq 2t + 1 \), any \( t \) errors can be corrected, meaning that there is a unique \( v \in C \) with \( wt(w - v) \leq t \).

A vector has at most \( m \) non-zero entries if and only if all the distinct \( m + 1 \) products of its entries are zero. This simple result was first exploited in the context of coding theory by De Boer and Pellikaan ([6]). Furthermore, one can translate the syndrome decoding algorithm, which is a widely used algorithm based on the method expressed above, into the language of varieties (called syndrome varieties), and use computational algebraic techniques (such as Gröbner bases) to find the errors and the nearest neighbors of a received message: see [6] (for cyclic codes) and [3] (for a general approach and with great application to error-correcting messages received through MDS codes).

The basic idea of our strategy to error-correct any message is the following: to the generating matrix of our linear code, augment the received message as a new row. This new matrix is the generating matrix for a new linear code, and under certain conditions (see the two bullets above) errors in the transmission become codewords of minimum weight in this new linear code (see Corollary [2,3]). We then use techniques from [13], that consist of saturation of ideals and primary decomposition, to determine these special codewords. When good messages are received (meaning vectors with unique nearest neighbor), both of these techniques are incorporated into one simple operation: colon a certain ideal by a power of a variable.

Finding the minimum distance of a linear code is computationally expensive, and in these notes we assume that this parameter has already been computed, either by the method of [6] (Gröbner bases or recursive calculation of heights of some ideals), by the debatably simpler method of
(see Section 3 for more details), or by some other procedure. We do not claim that our colon ideal method improves any existing algorithms; it would be rather difficult to achieve this considering the extensive work done in Gröbner bases type algorithms. But these approaches lack a theoretical perspective that whenever it is present turns out to be quite useful: here we are thinking about the nice homological properties of defining ideals of star configurations which can be obtained immediately from the theoretical results concerning MDS codes (see the first subsections of [8]). Our ultimate goal is to have a deeper theoretical understanding of this new method of error-correction, and to extend the homological study (i.e., graded free resolution) to more general ideals than the ideals defining star configurations, at the same time keeping the similar coding theoretical flavor. At the end one can discover that the results presented are in line with the theme of the landmark paper of Eisenbud and Goto on modules with linear free resolutions, [7].

2. ERRORS AS CODEWORDS OF MINIMUM WEIGHT

Let $C$ be an $[n, k, d]$—linear code with generating matrix $G$ as in the introduction. Suppose that a message $w = (w_1, w_2, \ldots, w_n) \in \mathbb{K}^n$ is received.

Create a new linear code $C^w$ with generating matrix

$$G^w := \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \\ w_1 & w_2 & \cdots & w_n \end{pmatrix}.$$

Observe that $G^w$ is created from the generator matrix $G$ of $C$ by augmenting the extra row $w$; a code with such a generating matrix is called augmented code.

Let $d_w := \min\{wt(\epsilon)|\epsilon \in \mathbb{K}^n \text{ with } w - \epsilon \in C\}$.

Two codewords are called projectively equivalent if they differ by multiplication by a non-zero scalar, and such an equivalence class, denoted with square brackets, is called a projective codeword. For any linear code $D$, denote with $PD(u)$ the set of projective codewords of weight $u$ in $D$.

The next result is somewhat folklore in coding theory (it seems that it appears in [1]), but for the sake of completeness we present it in the form we will use further in the article, with a complete simple proof.

**Theorem 2.1.** Let $w \notin C$. Then, the nearest neighbors of $w$ in $C$ (i.e., $v \in C$ such that $wt(w - v)$ is minimized) are in one-to-one correspondence with the projective codewords of weight $d_w$ in $C^w$ but not in $C$. 
Proof. First observe that \( w \notin C \) is equivalent to \( d_w \geq 1 \).

Consider the function

\[ \Phi : \{ \text{nearest neighbors of } w \in C \} \to \mathbb{P}C^w(d_w) \setminus \mathbb{P}C(d_w), \]

given by \( \Phi(v) = [w - v] \).

- **\( \Phi \) is well-defined:** Let \( v \) be a nearest neighbor of \( w \in C \). Then \( v \) minimizes \( \text{wt}(w - v) \), and so \( \text{wt}(w - v) = d_w \). It is obvious that \( w - v \in C^w \), as it is a linear combination of the rows of \( G^w \). If \( [w - v] = [v'] \) with \( v' \in C \), then \( w - v = \mu v' \), for some \( \mu \in \mathbb{K} \setminus \{0\} \), and hence \( w = v + \mu v' \in C \), a contradiction.

- **\( \Phi \) is injective:** If \( \Phi(v_1) = \Phi(v_2) \), then \( [w - v_1] = [w - v_2] \). Hence \( w - v_1 = \mu(w - v_2) \), for some \( \mu \neq 0 \) in \( \mathbb{K} \). If \( \mu = 1 \), then obviously \( v_1 = v_2 \). Otherwise, one has

\[ w = \frac{1}{\mu - 1}(\mu v_2 - v_1) \in C, \]

a contradiction.

- **\( \Phi \) is surjective:** Let \( \epsilon \in C^w - C \) with \( \text{wt}(\epsilon) = d_w \). We have that

\[ \epsilon = \lambda w + v, \]

for some \( v \in C \) and \( \lambda \neq 0 \) (otherwise, \( \epsilon \in C \)). Since \( \text{wt}(\frac{1}{\lambda} \epsilon) = \text{wt}(\epsilon) = d_w \), then \( v' := -\frac{1}{\lambda} v \in C \) is a nearest neighbor of \( w \) since \( \text{wt}(w - v') = d_w \), the minimum possible. Obviously

\[ \Phi(v') = [w - v'] = [-\frac{1}{\lambda} \epsilon] = [\epsilon], \]

and the proof is complete. \( \Box \)

**Remark 2.2.** It should be noted that Theorem 2.1 can be “extended” to the situation of \( w \in C \). In this instance \( C^w = C \), and \( d_w = 0 \). Since \( w \in C \), it is its own nearest neighbor. This corresponds to the only codeword in \( C = C^w \) of weight equal to \( d_w = 0 \), namely the zero vector, which can be written as \( w - w \).

Theorem 2.1 is particularly useful when \( w \notin C \) is a message received such that there exist \( v \in C \) with \( \text{wt}(w - v) \leq d - 1 \). This is the situation in the first bullet of the result presented in the Introduction.

**Corollary 2.3.** With respect to the notation used previously, if \( d_w \leq d - 1 \), then \( C^w \) is an \([n, k+1, d_w]\)-linear code, and therefore the nearest neighbors of \( w \) in \( C \) (hence the errors) are in one-to-one correspondence with the projective codewords of minimum weight of \( C^w \).

Proof. Since there are no codewords in \( C \) of weight \( d_w \), the set \( \mathbb{P}C(d_w) \) is empty.
$w \notin C$ assures that the dimension of $C^w$ is $k + 1$, and the minimality of $d_w$ assures that $C^w$ has minimum distance $d_w$. The result then follows from Theorem 2.1. □

**Remark 2.4.** The second bullet of the result in the Introduction translates into the following: if $1 \leq d_w \leq \lfloor (d - 1)/2 \rfloor$, then $|P C^w(d_w)| = 1$, meaning that $C^w$ has exactly one projective codeword of minimum weight. In the next section we will show that it is possible to avoid some of the computational challenges associated with calculating this codeword.

Until then, one can determine immediately from this projective codeword the error in $w$. This projective codeword is $[\lambda_1, \ldots, \lambda_k, \lambda]$, where $\lambda_i \in \mathbb{K}$ and $\lambda \neq 0$ (otherwise $x \in C$). So $[x]$ can be thought as the projective point $[\lambda_1, \ldots, \lambda_k, \lambda]$ in $\mathbb{P}^k$, and then the error in $w$ is the (affine) representative of this point in the affine open patch given by taking the last coordinate to be 1.

### 2.1. Counting the projective codewords of minimum weight

Theorem 2.1 suggests a recursive method of counting projective codewords of minimum weight.

Let $C$ be an $[n, k, d]$-linear code with generating matrix $G$. Let $j \in \{1, \ldots, k\}$ and let $C_j$ be the linear code with generating matrix $G_j$ obtained by removing row $j$ from $G$. Then, $C_j$ has length $n$ and dimension $k - 1$. Denote by $d_j$ its minimum distance. Since $C_j \subseteq C$, one has

$$d_j \geq d.$$  

Letting $\alpha_d(C)$ be the number of projective codewords of minimum weight of $C$, and denoting by $\text{n.n.}(w, C)$ the number of nearest neighbors in $C$ of a $w \notin C$, one has

**Corollary 2.5.** Let $r_j(G)$ denote the $j$--th row of $G$.

1. If $d_j > d$, then $\alpha_d(C) = \text{n.n.}(r_j(G), C_j)$.
2. If $d_j = d$, then $\alpha_d(C) = \alpha_d(C_j) + \text{n.n.}(r_j(G), C_j)$.

**Proof.** First, since $G$ is a $k \times n$ matrix of rank $k$, $r_j(G) \notin C_j$.

Write

$$\alpha_d(C) = [\alpha_d(C) - \alpha_d(C_j)] + \alpha_d(C_j).$$

The expression in brackets counts the number of projective codewords of weight $d$ in $C$ but not in $C_j$.

Setting $w = r_j(G)$ in Theorem 2.1, since $C = (C_j)_w$ one has

$$\alpha_d(C) - \alpha_d(C_j) = \text{n.n.}(r_j(G), C_j).$$
Hence,
\[ \alpha_d(C) = \alpha_d(C_j) + n. n. (r_j(G), C_j). \]
If \( d_j > d \), then \( C_j \) cannot not contain any of the codewords of weight \( d \), and so \( \alpha_d(C_j) = 0 \), giving
\[ \alpha_d(C) = n. n. (r_j(G), C_j). \]
\[ \square \]

Note that if one denotes by \( A_d(C) \) the number of codewords of weight \( d \) in \( C \), if \( \mathbb{K} \) is a finite field with \( q \) elements, then \( A_d(C) = (q - 1)\alpha_d(C) \).

Corollary 2.5 has a Commutative Algebraic translation that will be presented at the beginning of the next section.

3. USING COLON IDEALS TO ERROR-CORRECT MESSAGES

At the beginning of this section we briefly describe the method presented in [13] to obtain information about projective codewords of minimum weight from the commutative algebraic point of view.

Let \( C \) be an \([n, k, d]\)–linear code with generating matrix \( G \) of size \( k \times n \). To each column \( j \) of \( G \) we associate a homogeneous linear form \( L_j \) in \( R:= \mathbb{K}[x_1, \ldots, x_k] \) with coefficients being the entries in the corresponding column
\[ L_j = a_{1j}x_1 + a_{2j}x_2 + \cdots + a_{kj}x_k. \]
Then, create the ideals
\[ I_s(C) = \langle \{L_{j_1} \cdots L_{j_s}\}_{1 \leq j_1 < \cdots < j_s \leq n} \rangle \subset R. \]
[13, Theorem 3.1] shows that \( d \) is the maximum integer \( s \) such that the \( \mathbb{K} \)–vector subspace of \( R_s \) spanned by the generators of \( I_s(C) \) has dimension \( (k+s-1) \).

Concerning projective codewords of minimum weight, by [13, Lemma 2.2], \( I_{d+1}(C) \) has primary decomposition
\[ I_{d+1}(C) = q_1 \cap \cdots \cap q_m \cap J, \]
where \( q_i \) are prime ideals in \( R \) each defining a point in \( \mathbb{P}^{k-1} \), and \( J \subset R \) with \( \sqrt{J} = \langle x_1, \ldots, x_k \rangle \). The homogeneous coordinates of each point \( V(q_i) \in \mathbb{P}^{k-1} \) give the coefficients in the linear combination of the rows of \( G \) that equals a projective codeword of weight \( d \).

From this perspective, there are two immediate consequences

- The number of projective codewords of minimum weight equals the degree of the ideal \( I_{d+1}(C) \) (see [13, Corollary 2.3]), i.e.,
\[ m = \deg(I_{d+1}(C)) = \alpha_d(C). \]

\[ ^1 \text{For background on commutative algebra we suggest [5] and [12].} \]
Because the multiplicity of each \( q_i \) is one, finding \( q_1 \cap \cdots \cap q_m \), and hence finding the projective codewords of minimum weight, it is enough to saturate the ideal \( I_{d+1}(C) \) rather than computing its radical. In general, for an ideal \( I \subset R = \mathbb{K}[x_1, \ldots, x_k] \), the saturation of \( I \) is \( \text{sat}(I) = \{ f \in R | f \in I : (x_1, \ldots, x_k)^n(f) \text{ for some } n(f) \geq 1 \} = I : (x_1, \ldots, x_k)^\infty \).

To find projective codewords of minimum weight, one could solve the ideal \( I_{d+1}(C) \) using Gröbner bases (as [6] and [3] do), or find a primary decomposition for \( \text{sat}(I_{d+1}(C)) \); both methods are computationally expensive. Nevertheless, the Commutative Algebraic analog of Corollary 2.5 is the following:

**Corollary 3.1.** In the notations of Corollary 2.5 one has

\[ \text{n.n.}(r_j(G), C_j) = \deg(I_{d+1}(C) : x_j). \]

**Proof.** Consider the following classical exact sequence of graded \( R \text{-modules} \)

\[ 0 \longrightarrow \frac{R}{I_{d+1}(C) : x_j} \xrightarrow{x_j} \frac{R}{I_{d+1}(C)} \longrightarrow \frac{R}{I_{d+1}(C) + \langle x_j \rangle} \longrightarrow 0. \]

If we denote \( A = R/\langle x_j \rangle = \mathbb{K}[x_1, \ldots, \hat{x}_j, \ldots, x_k] \), then one has the isomorphism

\[ \frac{R}{I_{d+1}(C) + \langle x_j \rangle} \cong \frac{A}{I_{d+1}(C_j)}. \]

Hilbert polynomials (which are by definition the Hilbert function in sufficiently large degrees) are additive under exact sequences, so one has

\[ HP(\frac{R}{I_{d+1}(C) : x_j}, t - 1) + HP(\frac{A}{I_{d+1}(C_j)}, t) = HP(\frac{R}{I_{d+1}(C)}, t). \]

Since our ideals define projective schemes of dimensions \( \leq 0 \), the Hilbert polynomial equals the degree of the corresponding ideals. So one has that

\[ \deg(I_{d+1}(C) : x_j) + \deg(I_{d+1}(C_j)) = \deg(I_{d+1}(C)). \]

From [13, Theorem 3.1], for any \( [n', k', d'] \text{-linear code} \ D, I_j(D) = \langle x_1, \ldots, x_{k'} \rangle^j \text{ if and only if } j \leq d'. \) The degree of a power of a maximal ideal (in fact of any Artinian ideal) is zero. So the result follows now immediately from Corollary 2.5. \( \Box \)

We return to the situation of Section 2, Corollary 2.3: \( 1 \leq d_w \leq d - 1. \)

With regard to saturations, we have the following lemma:

**Lemma 3.2.** Consider \( I_{d_w+1}(C^w) \subset S := R[T] = \mathbb{K}[x_1, \ldots, x_k, T] \). If \( 1 \leq d_w \leq d - 1 \), then there exists a positive integer \( u \geq 1 \) such that

\[ \text{sat}(I_{d_w+1}(C^w)) = I_{d_w+1}(C^w) : T^u. \]
Proof. We have
\[ I_{d+1}(C_w) = \text{sat}(I_{d+1}(C_w)) \cap J, \]
where \( q_i \) are prime ideals in \( S \) and \( J \subset S \) with \( \sqrt{J} = \langle x_1, \ldots, x_k, T \rangle \). Then there exists a positive integer \( u \geq 1 \) for which \( Tu \in J \).

\( T \), and therefore \( Tu \), is a non-zero divisor in \( S/\bar{q}_1 \cap \cdots \cap \bar{q}_m \), since otherwise one of the points \( V(\bar{q}_i) \) would have its last coordinate 0, meaning that there would be a codeword of \( C_w \) of weight \( \leq d - 1 \) which is a linear combination of the first \( k \) rows of \( G_w \) and hence a codeword of \( C \).

Then
\[ I_{d+1}(C_w) : Tu = (\text{sat}(I_{d+1}(C_w)) : Tu) \cap (J : Tu) = \text{sat}(I_{d+1}(C_w)), \]
and the proof is complete. \( \square \)

It is desirable to have an upper bound \( v \) for the \( u \) above that depends only on \( n, k, d \) and/or \( d_w \), because then \( I_{d+1}(C_w) : Tu = I_{d+1}(C_w) : Tu \). Then, one could avoid using a recursive method to find the saturation. Finding such an upper bound is equivalent to finding an upper-bound for the index of saturation and, consequently, to finding an upper bound for the Castelnuovo-Mumford regularity. It is well known that the regularity provides an upper bound for the complexity of Gröbner basis algorithms that solve an ideal, and this is rather difficult to present. In any instance, we believe that this colon-ideal method looks quite easy to read and implement even for non-experts.

Example 3.3. Let us consider the linear code over \( \mathbb{F}_2 \) with generating matrix
\[
G = \begin{pmatrix}
1 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 1
\end{pmatrix}.
\]

Suppose the message \( w = (0, 1, 1, 1, 0, 0) \) is received.

One has
\[
G^w = \begin{pmatrix}
1 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 0
\end{pmatrix}.
\]
In \( \mathbb{P}^3 \), we have the six linear forms corresponding to the columns of \( G^w \):

\[
\begin{align*}
L_1 & := x \\
L_2 & := y + T \\
L_3 & := z + T \\
L_4 & := x + y + T \\
L_5 & := x + z \\
L_6 & := y + z.
\end{align*}
\]

Create

\[ I_2(C^w) = \langle \{L_i L_j\} \rangle_{1 \leq i < j \leq 6} \].

For the next computations we use Macaulay2 ([9]). Calculating heights gives \( \text{ht}(I_2(C^w)) = 3 \) and \( \text{ht}(I_1(C^w)) = 4 \), so by [6] one gets that

\[ d_w = 1 = (d - 1)/2. \]

We have

\[ I_2(C^w) : T = \langle x, y + T, z + T \rangle. \]

This is the ideal of the projective point \( P_w := [0, -\lambda, -\lambda, \lambda] \in \mathbb{P}^3, \lambda \neq 0. \)

The projective codeword of minimum weight is

\[ 0 \cdot r_1(G^w) + (-\lambda) \cdot r_2(G^w) + (-\lambda) \cdot r_3(G^w) + \lambda \cdot r_4(G^w) = (0, 0, 0, -\lambda, -2\lambda). \]

Since this is over \( \mathbb{F}_2 \), we obtain the precise error to be \( (0, 0, 0, 0, 1, 0) \).

If \( \deg(I_{d_w+1}(C^w)) > 1 \), then \( w \) has at least two nearest neighbors in \( C \), and in practice the message is requested to be sent again. So we will only consider the case when \( \deg(I_{d_w+1}(C^w)) = 1 \), meaning that \( \text{sat}(I_{d_w+1}(C^w)) \) consists of just one prime ideal, and finding its primary decomposition becomes superfluous. So for the remaining part of this section we assume the primary decomposition

\[ I_{d_w+1}(C^w) = \overline{q} \cap \overline{J} \subset S := \mathbb{K}[x_1, \ldots, x_k, T], \]

where \( \overline{q} \subset S \) is a prime ideal of codimension (i.e., height) \( k \) generated by linear forms and \( \sqrt{J} = \langle x_1, \ldots, x_k, T \rangle. \) Note that if \( 1 \leq d_w \leq [(d - 1)/2] \) this is always the case.

3.1. Error-correction of good messages through MDS codes. If \( C \) is MDS (i.e., \( d = n - k + 1 \)), the next result calculates the smallest \( u \) such that \( I_{d_w+1}(C^w) : T^u = \overline{q}. \) It is clear that \( u \geq d_w; \) otherwise \( T^u x_i \in I_{d_w+1}(C^w) \) has degree \( \leq d_w \) which is impossible since \( I_{d_w+1}(C^w) \) is generated in degrees \( d_w + 1 \).
Theorem 3.4. Let $C$ be an $[n, k, d]$–MDS code with $d = n - k + 1 \geq 3$. Let $w$ be a message with $1 \leq d_w \leq \lfloor (d - 1)/2 \rfloor$. Then
\[ I_{d_w + 1}(C^w) : T^{d_w} = \bar{q}. \]

Proof. Let $w = v + \epsilon$ with $v \in C$ and $\epsilon \in \mathbb{K}^n$ with $wt(\epsilon) = d_w$. Let $G$ be the generating matrix of $C$. Then $v \in C$ is a linear combination of the rows of $G$. Reducing the last row of $G^w$ by the coefficients of this linear combination one obtains $G'$ which is also a generating matrix of $C^w = C'$. So we can assume that $w = \epsilon$. Furthermore, after an appropriate permutation of the columns of $G$ and consequently of $G^w$ (i.e., of $G'$), we can assume that $w$ has the canonical form
\[ w = (0, \ldots, 0, a_{n-d_w+1}, a_{n-d_w+2}, \ldots, a_n), \text{ where } a_i \neq 0. \]
Because of this, $I_{d_w + 1}(C^w) = \bar{q} \cap J$ has $\bar{q} = \langle x_1, \ldots, x_k \rangle \subset S := \mathbb{K}[x_1, \ldots, x_k, T]$.

We denote with $L_i \in S, i = 1, \ldots, n$ the linear forms dual to the columns of $G^w$, and with $\ell_j \in R := \mathbb{K}[x_1, \ldots, x_n], i = 1, \ldots, n$ the linear forms dual to the columns of $G$. We have
\begin{align*}
L_i &= \ell_i, \text{ for } i = 1, \ldots, n-d_w \\
L_j &= \ell_j + a_j T, \text{ for } j = n-d_w+1, \ldots, n.
\end{align*}
We prove the result by induction on $d \geq 3$.

Case $d = 3$; base case. Then $n = k + 2$ and $d_w = 1$.
We have $L_1 = \ell_1, \ldots, L_{n-1} = \ell_{n-1}, L_n = T + \ell_n$, and therefore
\[ I_2(C^w) = \langle \{\ell_i \ell_j\}_{1 \leq i < j \leq n-1}, \ell_1 T + \ell_1 \ell_n, \ldots, \ell_{n-1} T + \ell_{n-1} \ell_n \rangle. \]
Since $C$ is an MDS code, any $k$ of the columns of $G$ are linearly independent and form a basis for $\mathbb{K}^k$. Then any product $\ell_i \ell_n, i = 1, \ldots, n-1$ can be written as
\[ \ell_i \ell_n = \ell_1 (c_1 \ell_{i_1} + \cdots + c_k \ell_{i_k}), \text{ where } i_j \neq n, i, \]
as $n = k + 2$. This means
\[ I_2(C^w) = \langle \{\ell_i \ell_j\}_{1 \leq i < j \leq n-1}, \ell_1 T, \ldots, \ell_{n-1} T \rangle. \]
Therefore
\[ \langle x_1, \ldots, x_k \rangle = \langle \ell_1, \ldots, \ell_{n-1} \rangle \subseteq I_2(C^w) : T. \]
The latter colon ideal is a subideal of $\bar{q} = \langle x_1, \ldots, x_k \rangle$ as $T$ is a nonzero divisor in $S/\bar{q}$. Hence we obtain equality throughout.

Case $d > 3$; induction step. Then $n > k+2$. If $d_w = 1$, the same argument as before applies, so assume that $d_w \geq 2$. 

Let $C' = C - \{\ell_n\}$ be the linear code obtained from $C$ by removing the last column in $G$. Since $d \geq 2$, the dimension of $C'$ is $k' = k$, and the minimum distance is $d' = d$ or $d' = d - 1$\footnote{We often make use of this technique of puncturing a code. For more details see \cite{11}, page 465.}. The length of $C'$ is $n' = n - 1$. Since $d' \leq n' - k' + 1 = n - k = d - 1$, then $d' = d - 1 = n - k$, and therefore, $C'$ is also an MDS linear code.

Let $w' = (0, \ldots, 0, a_{n-d_w+1}, \ldots, a_{n-1}) \in \mathbb{K}^{n-1}$, obtained from $w$ by removing the last entry. Then, by keeping with the notation used throughout this paper, we have

$$(C')^{w'} = C^w - \{L_n\}.$$ 

If $k_{w'}$ and $d_{w'}$ are the dimension and the minimum distance of this new linear code, respectively, since $d_w \geq 2$, then $k_{w'} = k' + 1 = k + 1$ and $d_{w'} = d_w$ or $d_{w'} = d_w - 1$. As the weight of $w' \in (C')^{w'}$ is $d_w - 1$, we must have

$$1 \leq d_{w'} = d_w - 1 \leq [(d - 1)/2] - 1 \leq [(d - 2)/2] = [(d' - 1)/2].$$

By the construction of $w'$ from $w$, we also have

$$\text{sat}(I_{d_{w'}+1}((C')^{w'})) = \langle x_1, \ldots, x_k \rangle = \bar{q}. \tag{1}$$

We can write

$$I_{d_{w'}+1}(C^w) = L_n \cdot I_{d_w}((C')^{w'}) + I_{d_{w'}+1}((C')^{w'}).$$

We write $L_n = a_n T + \ell_n$. Let $L_{i_1} \cdots L_{i_{d_w}} \in I_{d_w}((C')^{w'})$ be arbitrary. As $n-k = d-1 \geq 2d_w$, there exist indices $j_1, \ldots, j_k \in \{1, \ldots, n-d_w\} - \{i_1, \ldots, i_{d_w}\}$, and since $C$ is MDS, we can write $\ell_n$ as a linear combination of $\ell_{j_1} = L_{j_1}, \ldots, \ell_{j_k} = L_{j_k}$. This gives

$$\ell_n L_{i_1} \cdots L_{i_{d_w}} \in I_{d_{w'}+1}((C')^{w'}),$$

and so

$$I_{d_w}((C')^{w'}) \subseteq I_{d_{w'}+1}(C^w) : T.$$ 

By induction $\bar{q} \subseteq I_{d_{w'}+1}((C')^{w'}) : T^{d_{w'}}$, and hence the result. \hfill \Box

### 3.2. On the Castelnuovo-Mumford regularity of ideals generated by products of linear forms.

The Castelnuovo-Mumford regularity, or simply the regularity, of an ideal $I \subset S := \mathbb{K}[x_0, \ldots, x_n]$, denoted $\text{reg}(I)$, is one of the most important homological invariants in commutative algebra; as mentioned previously it can provide an upper bound on the complexity of the Gröbner basis algorithms that solve the ideal $I$. If

$$0 \to \oplus_i S(-b_{i,1}) \to \oplus_i S(-b_{i,t}) \to \cdots \to \oplus_i S(-b_{i,0}) \to I \to 0$$
is a graded minimal free resolution of $I$, then
\[
\text{reg}(I) = \max\{b_{i,j} - j\}.
\]

From the definition of $\text{sat}(I)$, the saturation of $I$ with respect to the maximal ideal, one usually defines a number called the saturation index (or index of saturation) of $I$, denoted here $\text{s.ind.}(I)$, which is the smallest integer $\delta$ such that $I_m = (\text{sat}(I))_m$ (the degree $m$ pieces) for all $m \geq \delta$.

The connection between these two numbers is
\[
\text{reg}(I) = \max\{\text{s.ind.}(I), \text{reg}(\text{sat}(I))\}.
\]

See [2] for more details.

In the assumptions of Theorem 3.4, since $d_w \geq 1$, and $I_{d_w+1}(C^w)$ is generated in degree $d_w + 1$, then
\[
\text{reg}(I_{d_w+1}(C^w)) \geq d_w + 1 > 1 = \text{reg}(\text{sat}(I_{d_w+1}(C^w))),
\]
giving that the regularity and the saturation index of $I_{d_w+1}(C^w)$ must coincide.

**Proposition 3.5.** Let $C$ be an $[n, k, d]$-MDS code with $d = n - k + 1 \geq 3$, and let $w \in \mathbb{K}^n$ be of weight $1 \leq m \leq [(d - 1)/2]$. Then
\[
\text{reg}(I_{m+1}(C^w)) = m + 1.
\]
In particular, $S/I_{m+1}(C^w)$ has a linear graded minimal free resolution.

**Proof.** Since $\text{wt}(w) = m \leq [(d - 1)/2]$, $C^w$ has a unique projective codeword of minimum weight $m$, namely $[w]$. After a permutation of the columns of the generating matrices of $C$ and $C^w$, similar to the beginning of proof of Theorem 3.4, we can assume
\[
w = (0, \ldots, 0, a_{n-m+1}, a_{n-m+2}, \ldots, a_n), \text{ where } a_i \neq 0,
\]
and
\[
I_{m+1}(C^w) = \langle x_1, \ldots, x_k \rangle \cap J \subset S := \mathbb{K}[x_1, \ldots, x_k, T].
\]

We will show that
\[
\bar{q} \subseteq I_{m+1}(C^w) : \langle x_1, \ldots, x_k, T \rangle^m.
\]
Given this result, if $f \in \bar{q}_{m+1}$, then $f = x_1g_1 + \cdots + x_kg_k$ for some $g_i \in \langle x_1, \ldots, x_k, T \rangle^m$. Therefore, $f$ is a degree $m + 1$ polynomial in $I_{m+1}(C^w)$. Since $I_{m+1}(C^w) \subset \bar{q}$, we have $(I_{m+1}(C^w))_{m+1} = \bar{q}_{m+1}$. So
\[
m + 1 \leq \text{reg}(I_{m+1}(C^w)) = \text{s.ind.}(I_{m+1}(C^w)) \leq m + 1.
\]

To show that $\bar{q} \subseteq I_{m+1}(C^w) : \langle x_1, \ldots, x_k, T \rangle^m$ is equivalent to showing
\[
\bar{q} \subseteq I_{m+1}(C^w) : \bar{q}^{m-i} \cdot T^i, \text{ for all } i = 0, \ldots, m.
\]
Claim: \( \bar{q} \subseteq I_{m+1}(C^\prime) : \bar{q}^m \). Let \( C'' \) be the puncturing of \( C \) at the last \( m \) columns of \( G \). Then \( C'' \) is an \([n-m, k, d-m]\)–MDS linear code. Since \( d-m \geq m+1 \), by [13, Theorem 3.1], one has
\[
I_{m+1}(C'') = \langle x_1, \ldots, x_k \rangle^{m+1} \subset R := \mathbb{K}[x_1, \ldots, x_k].
\]

Lifting up to \( S = R[T] \), since \( L_i = \ell_i, i = 1, \ldots, n-m \), in \( S \) we have
\[
\bar{q}^{m+1} \subset I_{m+1}(C'') S \subset I_{m+1}(C^w).
\]

This proves the claim.

With the Claim above we can prove the inclusion by using induction on \( d \geq 3 \).

Case \( d = 3 \); base case. Then \( m = 1 \). From the Claim above we have \( \bar{q} \subset I_2(C^w) : \bar{q} \). From Theorem 3.4 one also has \( \bar{q} = I_2(C^w) : T \). Hence the initial case of the induction is shown.

Case \( d \geq 4 \); induction step.
We use the same technique as in the proof of Theorem 3.4. Puncturing \( C \) at the last column, one obtains an MDS code \( C' \) with minimum distance \( d' = d-1 \), length \( n-1 \) and dimension \( k \). Also, removing the last coordinate in \( w \), one obtains \( w' \in \mathbb{K}^{n-1} \) of weight \( wt(w') = m' = m - 1 \). The inequalities
\[
2m' = 2m - 2 \leq d - 1 - 2 = d' - 2,
\]
allows the use of induction for \( C' \) and \( w' \), giving
\[
\bar{q} \subseteq I_{m'+1}((C')^w) : \bar{q}^{m'-i} \cdot T^i, \text{ for all } i = 0, \ldots, m'.
\]

In the proof of Theorem 3.4 we obtained
\[
I_m((C')^w) \subseteq I_{m+1}(C^w) : T.
\]
Putting everything together, with \( m = m' + 1 \), we have
\[
\bar{q} \subseteq I_{m+1}(C^w) : \bar{q}^{m-(i+1)} \cdot T^{i+1}, \text{ for all } i = 0, \ldots, m - 1,
\]
or equivalently (making \( i+1 = j \))
\[
\bar{q} \subseteq I_{m+1}(C^w) : \bar{q}^{m-j} \cdot T^j, \text{ for all } j = 1, \ldots, m.
\]
The Claim completes the proof. \( \square \)

As a corollary, we obtain the primary decomposition of the ideal defining the scheme of projective codewords of minimum weight. It is known that for any \([n, k, d]\)–linear code \( C \), if \( 1 \leq i \leq d \), \( I_i(C) = \langle x_1, \ldots, x_k \rangle^i \) (see [13, Theorem 3.1]), which leads naturally to the question of the the structure of \( I_i(C) \), for \( i \geq d + 1 \). In general, the embedded component of \( I_{d+1}(C) \) is not known or well understood. In the next result, we show that under some
special conditions the embedded component is in fact a power of the maximal ideal. This will immediately give us the graded minimal free resolution for this ideal. One should note that we obtain a very simple case of [10, Theorem 5.7].

**Corollary 3.6.** Let $C$ be an $[n, k, d]$-MDS code with $d \geq 3$. Let $w \in \mathbb{K}^n$ be a vector of weight $\text{wt}(w) = t \leq \lfloor (d - 1)/2 \rfloor$. Then,

$$I_{t+1}(C^w) = \bar{q} \cap \langle x_1, \ldots, x_k, T \rangle^t \subset S = \mathbb{K}[x_1, \ldots, x_k, T],$$

where $\bar{q} \subset S$ is a prime ideal of codimension $k$, generated by linear forms. Further, the graded minimal free resolution of $S/I_{t+1}(C^w)$ is

$$0 \rightarrow S^{\beta_{k+1}}(-(t + k + 1)) \rightarrow \cdots \rightarrow S^{\beta_1}(-(t + 1)) \rightarrow S,$$

where $\beta_i = (i+t-1)^{(k+i)}(t_i+1) - (k+1)$, for $i = 1, \ldots, k + 1$.

**Proof.** The first part is immediate since we showed in the proof of Proposition [5.5] that $(I_{t+1}(C^w))_{t+1} = \bar{q}_{t+1}$, and therefore $I_{t+1}(C^w) = \bar{q}_{t+1}$.

For the second part, let $I = I_{t+1}(C^w)$. We can also assume that $\bar{q} = \langle x_1, \ldots, x_k \rangle$. The primary decomposition above gives rise to the short exact sequence of $S$-modules

$$0 \rightarrow \frac{S}{I} \rightarrow \frac{S}{\langle x_1, \ldots, x_k \rangle} \oplus \frac{S}{\langle x_1, \ldots, x_k, T \rangle^t} \rightarrow \frac{S}{\langle x_1, \ldots, x_k, T^{t+1} \rangle} \rightarrow 0.$$

- Let $G_*$ be the graded minimal free resolution of $\frac{S}{\langle x_1, \ldots, x_k \rangle}$. Then $G_i = S^{a_i}(-i), a_i = \binom{k}{i}, i = 0, \ldots, k$ and $G_{k+1} = G_{k+2} = 0$.

- Let $H_*$ be the graded minimal free resolution of $\frac{S}{\langle x_1, \ldots, x_k, T \rangle^t}$. Then $H_i = S^{b_i}(-(t+i)), b_i = (t+i)^{(k+i)}(t_i+1), i = 1, \ldots, k+1$ and $H_0 = S$ and $H_{k+2} = 0$.

- Let $E_*$ be the graded minimal free resolution of $\frac{S}{\langle x_1, \ldots, x_k, T^{t+1} \rangle}$. Then $E_i = G_i \oplus G_{i-1}(-(t+1))$ and $E_0 = S$.

If $F_*$ is the minimal graded free resolution of $S/I$, with $F_0 = S$ and by convention $F_{-1} = 0$, the mapping cone on the short exact sequence above says that

$$F_i \oplus G_{i+1} \oplus H_{i+1}, i = -1, \ldots, k + 1,$$

are the free modules in a graded free resolution for $\frac{S}{\langle x_1, \ldots, x_k, T^{t+1} \rangle}$. Comparing this with the minimal graded free resolution $E_*$, there must be redundancies in the mapping cone. This gives

$$H_i = F_i \oplus G_{i-1}(-(t+1)), i = 1, \ldots, k + 1,$$

and so $\beta_i = b_i - a_{i-1}$.
Acknowledgement  The first author is supported by the Brian and Gayle Hill Fellowship awarded by the College of Science at University of Idaho.

REFERENCES

[1] A. Barg, Complexity issues in coding theory, in Handbook of Coding Theory, vol. 1, Elsevier Science, 1998, pp. 649–754.
[2] I. Bermejo, P. Gimenez, Saturation and Castelnuovo-Mumford regularity, J. Algebra, 303 (2006), pp. 592–617.
[3] S. Bulygin, R. Pellikaan, Bounded distance decoding of linear error-correcting codes with Gröbner bases, J. Symbolic Computation, 44 (2009), pp. 1626–1643.
[4] D. Cox, J. Little, D. O’Shea, Using Algebraic Geometry, Springer-Verlag, New York, 1998.
[5] D. Cox, J. Little, D. O’Shea, Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, Third Edition, Springer, New York, 2010.
[6] M. De Boer, R. Pellikaan, Grobner Bases for Codes, in Some Tapas of Computer Algebra, Springer, 1999, pp. 237–259.
[7] D. Eisenbud, S. Goto, Linear free resolutions and minimal multiplicity, J. Algebra, 88 (1984), pp. 89–133.
[8] A. Geramita, B. Harbourne, J. Migliore, Star configurations in $\mathbb{P}^n$, J. Algebra, 376 (2013), pp. 279–299.
[9] D. Grayson, M. Stillman, Macaulay2, a software system for research in algebraic geometry, Available at [http://www.math.uiuc.edu/Macaulay2/](http://www.math.uiuc.edu/Macaulay2/)
[10] J. Herzog, A. Simis, W. Vasconcelos, Approximation complexes of blowing-up rings, II, J. Algebra, 82 (1983), pp. 53–83.
[11] W. Huffman, V. Pless, editors, Handbook of Coding Theory Volumes 1 & 2, Elsevier Science B.V., Netherlands, 1998.
[12] R. Sharp, Steps in Commutative Algebra, Second Edition, Cambridge University Press, Cambridge, 2000.
[13] S. Tohaneanu, On the De Boer-Pellikaan method for computing minimum distance, J. Symbolic Computation, 45 (2010), pp. 965–974.