Gulf Journal of Mathematics ISSN: 2309-4966
Vol 18, Issue 2 (2024) 29-46 https://doi.org/10.56947/gjom.v18i2.2397

HEIGHTS OF ERROR-CORRECTING CODES

DARMOUN SABER[1*], ABDELMOUMEN KHALID[2] and BEN-AZZA HUSSAIN[3]

Abstract. In this work, we investigate the evaluation of odd polynomials P defined on a finite field on the class of error-correcting codes $\mathbf{C}$. We exploit the correspondence between codes and Tanner graphs. Thus, we formally define $P(\mathbf{C})$, a polynomial code. Then the new notion of height of a code emerges, whose properties are studied. We extended the lower bound of Tanner on the minimum distance of a code to the case of a polynomial code, by using spectral graph theory. Computer algebra software enable us to give numerical results to illustrate the theory of polynomial codes for various classes of error-correcting codes.

1. Introduction and preliminaries

The correspondence between graph theory and error-correcting codes theory is well known, in particular in Tanner graphs which are bipartite [9]. Let $\mathbf{C}$ be an $[n,k,d]_q$ linear code over $GF(q)$ with a parity check matrix $H = H(\mathbf{C})$ of size $r \times n$ where $r = n-k$, and a $k \times n$ generating matrix $G = G(\mathbf{C})$. Set $M = HH^T$ a symmetric $r \times r$ matrix and

$$A = \begin{bmatrix} 0 & H \\ H^T & 0 \end{bmatrix}. \tag{1.1}$$

The $(n+r)\times(n+r)$ matrix A may be seen as the adjacency matrix of a bipartite graph Γ equipped with a labeling on the edges $L : E\Gamma \to GF(q) - 0$. As observed by Tanner [9], there is a one-to-one correspondence between matrices H (hence linear codes $\mathbf{C}$) and bipartite graphs with a labeling L. We want to use the matrix A for a more general point of view and for a different perspectives, thinking of evaluating a polynomial $P(X) \in GF(q)[X]$ on this matrix and seeing what happens.

In this paper, we fix an odd polynomial $P(X) = \sum_{i=1}^{2\nu+1} a_i X^i \in GF(q)[X]$ such that for all even indices i, we have $a_i = 0$, and apply it to the matrix A. The choice of an odd polynomial is intended to keep us within the set of codes. In the first part, our aim is therefore to give a formal meaning to the code $P(\mathbf{C})$ through its parity check matrix, and we give some results on its parameters. This

Date: Received: Oct 28, 2024; Accepted: Nov 23, 2024.

* Corresponding author.

2020 *Mathematics Subject Classification.* Primary 11T71, 05C50; Secondary 11T06.

Key words and phrases. Polynomials in codes, Height of a linear code, Graph spectrum, Minimum distance.

has enabled us to look at the odd powers of a linear code $\mathbf{C}$ denoted by $\mathbf{C}^{(2\nu+1)}$ for a certain nonnegative integer ν. Therefore, we take the particular case of unitary monomials.

Due to the algebraic structure of code powers, we show that each code is contained in another of increasing power. This chain of inclusions influences the dimension k and the minimum distance d of the initial code. On the one hand, the dimension increases. On the other hand, the minimum distance decreases until it finally stops at a precise rank. It will later be called the height of a linear code $\mathbf{C}$, denoted $\mathbf{Ht}(\mathbf{C})$, and defined as a new notion of error-correcting codes.

An upper bound is given for the height in terms of the length n and the dimension k for any linear code. Another upper bound is given for the height in terms of the minimum distance d of the initial code $\mathbf{C}$ in the case where it decreases strictly with each inclusion step.

In the other part of this paper, our aim is to find a lower bound on the minimum distance of the code $\mathbf{C}^{(2\nu+1)}$ based on the spectral study of the matrix $(M^\nu H)^T M^\nu H$ constructed from the regular bipartite graph Γ of adjacency matrix A (1.1). Our strategy is based first on giving results relating the eigenvalues of the matrix $H^T H$ to those of the matrix $(M^\nu H)^T M^\nu H$. The rest is then technical focusing on the first and the second eigenvalues. An upper bound on the height of the code is afterwards given.

The plan to represent our ideas clearly is to first define the code $P(\mathbf{C})$ by calculating the matrix $P(A)$ and then using the same correspondence discussed above to find the parity check matrix of the new code. Then we will focus on the powers of the code and some related results in order to define the height of a code by giving its bounds. Subsequently, we discuss the bounds on the dimension and the minimum distance of the code $\mathbf{C}^{(2\nu+1)}$. Afterwards, we give some examples generated by the computer algebra system SAGE with both random and known codes, for which we give their heights.

In the second part, we conduct a spectral analysis to obtain results on eigenvalues and their use for the minimum distance of the code $\mathbf{C}^{(2\nu+1)}$ in order to generalize the result given by Tanner [9]. For more information and definitions on coding theory, graph theory and spectral graph theory, the reader is referred to [7, 5, 6, 10], [2], and [4, 3], respectively.

2. Main results

2.1. Polynomials In Codes.

Proposition 2.1. *Let $Q(X) = a_1 + a_3X + \cdots + a_{2\nu+1}X^\nu \in GF(q)[X]$. Then over $GF(q)$, we have*

$$P(A) = \begin{bmatrix} 0 & Q(M)H \\ H^T Q(M) & 0 \end{bmatrix},$$

where $Q(M) = a_1 I_r + a_3 M + \cdots + a_{2\nu+1} M^\nu$.

Proof. Let $\mathbb{K} = GF(q)$ and $\nu \in \mathbb{N}^*$. Let $P(X) \in \mathbb{K}_{2\nu+1}[X]$, where $\mathbb{K}_{2\nu+1}[X]$ represents the ring of polynomials of degrees at most $2\nu+1$ with coefficients in

$\mathbb{K}$, and let $P(X) = \sum_{i=1}^{2v+1} a_i X^i$ with $a_i = 0$ for all even indices i. By using the matrix:

$$A = \begin{bmatrix} 0 & H \\ H^T & 0 \end{bmatrix},$$

$H \in \mathcal{M}_{r,n}(\mathbb{K})$ is a parity check matrix of the $[n,k,d]_q$ linear code over $\mathbb{K}$.
We proceed by induction. For $\nu = 1$, we have $P(A) = a_1 A + a_3 A^3$, and

$$A^2 = \begin{bmatrix} HH^T & 0 \\ 0 & H^T H \end{bmatrix},$$
$$A^3 = \begin{bmatrix} 0 & HH^T H \\ H^T HH^T & 0 \end{bmatrix},$$

then,

$$\begin{aligned} P(A) &= \begin{bmatrix} 0 & a_1 H + a_3 HH^T H \\ a_1 H^T + a_3 H^T HH^T & 0 \end{bmatrix}, \\ &= \begin{bmatrix} 0 & (a_1 I_r + a_3 HH^T)H \\ H^T(a_1 I_r + a_3 HH^T) & 0 \end{bmatrix}. \end{aligned}$$

Since $M = HH^T$, we have

$$P(A) = \begin{bmatrix} 0 & (a_1 I_r + a_3 M)H \\ H^T(a_1 I_r + a_3 M) & 0 \end{bmatrix}.$$

We put $Q(M) = a_1 I_r + a_3 M$ where $Q(X) = a_1 + a_3 X \in \mathbb{K}_1[X]$
then for $\nu = 1$,

$$P(A) = \begin{bmatrix} 0 & Q(M)H \\ H^T Q(M) & 0 \end{bmatrix}.$$

For a certain $\nu \in \mathbb{N}^*$, we assume that

$$P(A) = \begin{bmatrix} 0 & Q(M)H \\ H^T Q(M) & 0 \end{bmatrix}, \tag{2.1}$$

for $P(X) \in \mathbb{K}_{2v+1}[X]$ and $Q(X) \in \mathbb{K}_\nu[X]$ with $Q(M) = a_1 I_r + a_3 M + ... + a_{2\nu+1} M^\nu$. Let's show for $\nu + 1$ that

$$P(A) = \begin{bmatrix} 0 & Q(M)H \\ H^T Q(M) & 0 \end{bmatrix}.$$

Let $P(X) \in \mathbb{K}_{2\nu+3}[X], P(X) = \sum_{i=1}^{2v+3} a_i X^i, a_i = 0$ for all even indices i.

We have $\forall\ n \in \mathbb{N}$,

$$A^{2n} = \begin{bmatrix} (HH^T)^n & 0 \\ 0 & (H^T H)^n \end{bmatrix},$$

then,

$$A^{2n+3} = A^{2n} \times A^3, \tag{2.2}$$

$$= \begin{bmatrix} 0 & (HH^T)^{n+1}H \\ (H^TH)^{n+1}H^T & 0 \end{bmatrix}. \tag{2.3}$$

$P(A) = \sum_{i=1}^{2\nu+3} a_iA^i$ with $a_i = 0$ for all even indices i, thus

$$P(A) = a_1A + a_3A^3 + ... + a_{2\nu+1}A^{2\nu+1} + a_{2\nu+3}A^{2\nu+3}.$$

The equations (2.1) and (2.3) imply,

$$P(A) = \begin{bmatrix} 0 & (\sum_{i=0}^{\nu} a_{2i+1}M^i)H + a_{2\nu+3}(HH^T)^{\nu+1}H \\ H^T(\sum_{i=0}^{\nu} a_{2i+1}M^i) + a_{2\nu+3}(H^TH)^{\nu+1}H^T & 0 \end{bmatrix}.$$

And since $(H^TH)^{\nu+1}H^T = H^T(HH^T)^{\nu+1}$, we have

$$P(A) = \begin{bmatrix} 0 & (\sum_{i=0}^{\nu} a_{2i+1}M^i + a_{2\nu+3}(HH^T)^{\nu+1})H \\ H^T(\sum_{i=0}^{\nu} a_{2i+1}M^i + a_{2\nu+3}(HH^T)^{\nu+1}) & 0 \end{bmatrix},$$

$$= \begin{bmatrix} 0 & (\sum_{i=0}^{\nu} a_{2i+1}M^i + a_{2\nu+3}M^{\nu+1})H \\ H^T(\sum_{i=0}^{\nu} a_{2i+1}M^i + a_{2\nu+3}M^{\nu+1}) & 0 \end{bmatrix},$$

hence,

$$P(A) = \begin{bmatrix} 0 & Q(M)H \\ H^TQ(M) & 0 \end{bmatrix}.$$

With $Q(X) \in \mathbb{K}_{\nu+1}[X], Q(M) = a_1I_r + a_3M + ... + a_{2\nu+1}M^v + a_{2\nu+3}M^{\nu+1}$. And so : $\forall\ \nu \in \mathbb{N}^*$ such that $P(X) = \sum_{i=1}^{2\nu+1} a_iX^i$ with $a_i = 0$ for all even indices i, we have

$$P(A) = \begin{bmatrix} 0 & Q(M)H \\ H^TQ(M) & 0 \end{bmatrix},$$

where $Q(M) = a_1I_r + a_3M + ... + a_{2\nu+1}M^\nu$. $\square$

This proposition and Tanner's observation allow to define the code $P(\mathbf{C})$ with the parity check matrix

$$H(P(\mathbf{C})) = Q(M)H.$$

The code $P(\mathbf{C})$ is formally denoted by

$$P(\mathbf{C}) = a_1\mathbf{C}\dot{+}\cdots\dot{+}a_{2\nu+1}\mathbf{C}^{(2\nu+1)}. \tag{2.4}$$

Definition 2.2. $P(\mathbf{C})$ is a linear code over $GF(q)$ defined by

$$P(\mathbf{C}) = \left\{x \in GF(q)^n / \, x(Q(M)H)^T = 0\right\}.$$

Remark 2.3. $P(\mathbf{C})$ is a vector subspace of $GF(q)^n$. In fact we have $P(\mathbf{C}) \subset GF(q)^n$ and it's a non-empty set since $0 \in P(\mathbf{C})$.
Let $\alpha, \beta \in GF(q)$ and $x, y \in P(\mathbf{C})$ then,

$$\begin{aligned}(\alpha x + \beta y)(Q(M)H)^T &= \alpha x(Q(M)H)^T + \beta y(Q(M)H)^T \\ &= 0 + 0 = 0.\end{aligned}$$

Then $\alpha x + \beta y \in P(\mathbf{C})$, consequently $P(\mathbf{C})$ is a vector subspace of $GF(q)^n$.

Notation 2.4. The power of the linear code $\mathbf{C}$ is denoted by $\mathbf{C}^{(2j+1)}$ for a certain nonnegative integer j. If $j = 0$, we have $\mathbf{C}^{(1)} = \mathbf{C}$.

Corollary 2.5. *Let j be a nonnegative integer, then the parity check matrix of $\mathbf{C}^{(2j+1)}$ is M^jH. In fact we have $H(P(\mathbf{C})) = Q(M)H$ with $Q(M) = a_1 I_r + a_3 M + \cdots + a_{2\nu+1}M^\nu$, hence we put $a_1 = a_2 = \cdots = a_{2\nu+1} = 0$ except $a_{2j+1} = 1$ for a certain nonnegative integer j. Thus $P(\mathbf{C}) = \mathbf{C}^{(2j+1)}$, then $H(\mathbf{C}^{(2j+1)}) = M^jH$ as $Q(M) = M^j$.*

Definition 2.6. For all nonnegative j, the $(2j+1)th$ power of the linear code $\mathbf{C}$ is defined by

$$\mathbf{C}^{(2j+1)} = \left\{x \in GF(q)^n / \, x(M^jH)^T = 0\right\}.$$

Remark 2.7. (Clarification)
If we consider the sequence of monomials $Q_\nu = a_\nu X^\nu$, where a_ν is a nonzero element of $GF(q)$, and denote $P_\nu(C)$ the code with the parity check matrix $H(P_\nu(\mathbf{C})) = Q_\nu(M)H$, then we have $P_\nu(\mathbf{C}) \subset P_{\nu+1}(\mathbf{C})$. Note that if we consider the code $P(\mathbf{C})$ associated with the polynomial $P(X) = \sum_{i=1}^{2\nu+1} a_i X^i$, with $a_{2\nu+1} \neq 0$, we haven't in general $P(\mathbf{C}) \subset P_\nu(\mathbf{C})$, and the code $P(\mathbf{C})$ is not the combination $\sum_{i=1}^{\nu} P_i(\mathbf{C})$ of subspaces. Thus the code $P(\mathbf{C})$ is not the code $P_\nu(\mathbf{C})$. This justifies the choice of notation $''\dot{+}''$ instead of $''+''$ in (2.4).

Proposition 2.8. *With the same previous notations we have :*

(1) $\mathbf{C} \subseteq P(\mathbf{C})$.
(2) $\mathbf{C} \subseteq \mathbf{C}^{(3)} \subseteq \cdots \subseteq \mathbf{C}^{(2\nu+1)} \subseteq \cdots$
(3) *For $j \neq l$, and $a, b \in GF(q)$, $H(a\mathbf{C}^{(2j+1)} \dot{+} b\mathbf{C}^{(2l+1)}) = aH(\mathbf{C}^{(2j+1)}) + bH(\mathbf{C}^{(2l+1)})$.*

Proof. (1) Let $x \in \mathbf{C}$, then

$$\begin{aligned} xH^T = 0 &\implies xH^TQ(M) = 0 \\ &\implies x(Q(M)H)^T = 0.\end{aligned}$$

Since $H(P(\mathbf{C})) = Q(M)H$, we have $x \in P(\mathbf{C})$, thus $\mathbf{C} \subseteq P(\mathbf{C})$.

(2) We proceed by induction to show that :

$$\forall\, j \geq 0, \mathbf{C}^{(2j+1)} \subseteq \mathbf{C}^{(2j+3)}.$$

For $j=0$, $\mathbf{C} \subseteq \mathbf{C}^{(3)}$ by the property (1).
We supposed that $\mathbf{C}^{(2j+1)} \subseteq \mathbf{C}^{(2j+3)}$ for a certain nonnegative integer j, and let's show that $\mathbf{C}^{(2j+3)} \subseteq \mathbf{C}^{(2j+5)}$. We have for all $x \in \mathbf{C}^{(2j+1)}$, $x \in \mathbf{C}^{(2j+3)}$, then

$$\begin{aligned} x(M^{j+1}H)^T = 0 &\implies xH^T M^{j+1} = 0 \\ &\implies xH^T M^{j+1} M = 0 \\ &\implies xH^T M^{j+2} = 0 \\ &\implies x(M^{j+2}H)^T = 0 \\ &\implies x \in \mathbf{C}^{(2j+5)}. \end{aligned}$$

Thus $\forall\ j \geq 0, \mathbf{C}^{(2j+1)} \subseteq \mathbf{C}^{(2j+3)}$. By changing j over $\mathbb{N}$ we have $\mathbf{C} \subseteq \mathbf{C}^{(3)} \subseteq \cdots \subseteq \mathbf{C}^{(2\nu+1)} \subseteq \cdots$

(3) We know that $H(P(\mathbf{C})) = Q(M)H$, we put for $j \neq l$, and $a, b \in GF(q)$,

$$P(\mathbf{C}) = a\mathbf{C}^{(2j+1)} \dot{+} b\mathbf{C}^{(2l+1)}.$$

Then,

$$\begin{aligned} H(P(\mathbf{C})) &= (aM^j + bM^l)H, \\ &= aM^jH + bM^lH, \\ &= aH(\mathbf{C}^{(2j+1)}) + bH(\mathbf{C}^{(2l+1)}). \end{aligned}$$

□

Remark 2.9. In the above chain of inclusions we have the length of codes remains stable. The dimension is increasing while the minimum distance is decreasing.

Remark 2.10. (Distance stability)
In the chain of inclusions of odd powers of the code $\mathbf{C}$, the distance stabilizes in a certain rank. In fact from the above proposition we have $\mathbf{C}^{(2j+1)} \subseteq \mathbf{C}^{(2l+1)}$ for all nonnegatives $l \geq j$.
Let us denote by k_j the dimension of $\mathbf{C}^{(2j+1)}$ for $j \in \mathbb{N}^*$. We have,

$$\begin{aligned} k_j \leq k_l &\iff n - k_l \leq n - k_j \\ &\iff rank(H(\mathbf{C}^{(2l+1)})) \leq rank(H(\mathbf{C}^{(2j+1)})). \end{aligned}$$

Since the Singleton bound $d \leq n-k+1$ and as the dimension in the chain of codes increases, then the rank of their parity check matrices decreases, it stabilizes. In this case the chain of inclusions stops because we will find the same code that repeats itself.

Definition 2.11. (Height of a code)
Let $\mathbf{C}$ be an $[n,k,d]_q$ linear code over $GF(q)$. The height of the code $\mathbf{C}$ is denoted by $\mathbf{Ht}(\mathbf{C})$ and it is defined by :

$$\mathbf{Ht}(\mathbf{C}) = max\left\{ i \in \mathbb{N} \;/\; \mathbf{C}^{(2i+1)} = \mathbf{C}^{(2i+3)} \right\}.$$

It is the smallest nonnegative integer r verifying :

$$\forall\ j > r,\ \mathbf{C}^{(2r+1)} = \mathbf{C}^{(2j+1)}.$$

Remark 2.12. (1) The height of the code $\mathbf{C}$ can be seen as the length of the following chain

$$\mathbf{C} \subseteq \mathbf{C}^{(3)} \subseteq \cdots \subseteq \mathbf{C}^{(2\nu+1)} \subseteq \cdots$$

(2) The height of the code $\mathbf{C}$ is its stability order.
(3) $\mathbf{Ht}(\mathbf{C}) = 0$ if and only if $\mathbf{C} = \mathbf{C}^{(2i+1)}\ \forall\, i \in \mathbb{N}$.

Proposition 2.13. *$\boldsymbol{Ht}(\mathbf{C}) = 0$ if and only if $M = HH^T$ is invertible.*

Proof. Let i be a nonnegative integer, $x \in \mathbf{C}^{(2i+1)}$ and $M = HH^T$. Then $x(M^iH)^T = xH^TM^i = 0$.
M is invertible implies $xH^T = 0$, hence $x \in \mathbf{C}$. Thus $\mathbf{Ht}(\mathbf{C}) = 0$.
Reciprocally, we assume that $\mathbf{Ht}(\mathbf{C}) = 0$ i.e. $\mathbf{C} = \mathbf{C}^{(3)}$ and we suppose that M is not invertible. Then we have $rank(M) < n - k$ (M is not a full rank matrix), thus $rank(MH) \leq min(rank(M), rank(H)) = rank(M)$. Consequently, $dim(\mathbf{C}^{(3)}) = n - rank(MH) > k$. Absurd as $dim(\mathbf{C}) = k$. □

Remark 2.14. If $M = HH^T = 0$, then $\mathbf{C}^{(3)} = GF(q)^n$.

We need the following lemma.

Lemma 2.15. *For each nonnegative $j < \boldsymbol{Ht}(\mathbf{C})$, $\mathbf{C}^{(2j+1)}$ is strictly included in $\mathbf{C}^{(2j+3)}$.*

Proof. Let $r = \mathbf{Ht}(\mathbf{C})$, and $j < r$ such that $\mathbf{C}^{(2j+1)} = \mathbf{C}^{(2j+3)}$.
Then $M^jH = M^{j+1}H$, so by multiplying the equality by the powers of M we get $M^jH = M^rH = M^{r+1}H = ...$, thus $\mathbf{C}^{(2j+1)} = \mathbf{C}^{(2r+1)} = \mathbf{C}^{(2r+3)} = ...$
This implies $j = \mathbf{Ht}(\mathbf{C})$. Contradiction □

Proposition 2.16. *For any linear code $\mathbf{C}$ of length n and dimension k, we have*

$$\boldsymbol{Ht}(\mathbf{C}) \leq n - k.$$

Proof. In fact we have $n \geq k$ for $\mathbf{C}$, then by the lemma 2.15, for $\mathbf{C}^{(3)}$ we have at least $n \geq k + 1$,
for $\mathbf{C}^{(5)}$ we have at least $n \geq k + 2$, and so forth until $\mathbf{C}^{(2\mathbf{Ht}(\mathbf{C})+1)}$ that we have $n \geq k + \mathbf{Ht}(\mathbf{C})$. □

Proposition 2.17. *Let $\mathbf{C}$ be an $[n, k, d]_q$ linear code over $GF(q)$. If the minimum distance decreases by at least one in each increasing power of the code $\mathbf{C}$, then*

$$\boldsymbol{Ht}(\mathbf{C}) \leq d - 1.$$

Proof. We have in this chain $\mathbf{C} \subseteq \mathbf{C}^{(3)} \subseteq \cdots \subseteq \mathbf{C}^{(2\nu+1)} \subseteq \cdots \subseteq \mathbf{C}^{(2\mathbf{Ht}(\mathbf{C})+1)}$. As the distance decreases as least by one in every move, then if $\mathbf{Ht}(\mathbf{C}) \geq d$ we have the distance corresponding to $\mathbf{C}^{(2\mathbf{Ht}(\mathbf{C})+1)}$ decreased at least by d, so $d(\mathbf{C}^{(2\mathbf{Ht}(\mathbf{C})+1)})$ is less or equal to 0, which impossible since $\mathbf{C}^{(2\mathbf{Ht}(\mathbf{C})+1)}$ is different to the zero code. Then the result. □

Remark 2.18. We can see this result in two different ways :

(1) If we take a known $[n, k, d]_q$ linear code over $GF(q)$, we can get an idea of its stability rank since it can't exceed $d - 1$.

(2) If we take a code that we only know its parity check matrix, we iterate to stability and we get an idea about its minimum distance which must be greater than the height plus 1.

Proposition 2.19. *Let* $\mathbf{C}$ *be an* $[n,k,d]_q$ *linear code over* $GF(q)$. *If* $j < \boldsymbol{Ht}(\mathbf{C})$, *then*

$$dim(\mathbf{C}^{(2j+1)}) \geq dim(\mathbf{C}) + j.$$

Proof. By induction on j.
The assertion is true for $j = 0$.
We suppose that the assertion is true for a certain $j \in \mathbb{N}$, and we provide that

$$dim(\mathbf{C}^{(2j+3)}) \geq dim(\mathbf{C}) + j + 1.$$

We have by the lemma 2.15 for $j < \mathbf{Ht}(\mathbf{C})$, $\mathbf{C}^{(2j+1)} \subset \mathbf{C}^{(2j+3)}$, then

$$dim(\mathbf{C}^{(2j+3)}) \geq dim(\mathbf{C}^{(2j+1)}) + 1.$$

Furthermore,

$$dim(\mathbf{C}^{(2j+1)}) \geq dim(\mathbf{C}) + j.$$

Then

$$dim(\mathbf{C}^{(2j+3)}) \geq dim(\mathbf{C}) + j + 1.$$

Hence the result. $\square$

Corollary 2.20. $\forall\, j \geq \boldsymbol{Ht}(\mathbf{C})$, $dim(\mathbf{C}^{(2j+1)}) \geq dim(\mathbf{C}) + \boldsymbol{Ht}(\mathbf{C})$.

Proposition 2.21. *Let* $\mathbf{C}$ *be an* $[n,k,d]_q$ *linear code over* $GF(q)$. *If the minimum distance decreases by at least one in each increasing power of the code* $\mathbf{C}$, *and if* $j < \boldsymbol{Ht}(\mathbf{C})$, *then*

$$1 \leq d(\mathbf{C}^{(2j+1)}) \leq d(\mathbf{C}) - j.$$

Proof. By induction on j
for $j = 0$ we have the assertion is true.
We suppose that the assertion is true for a certain $j \in \mathbb{N}$, and we provide that

$$1 \leq d(\mathbf{C}^{(2j+3)}) \leq d(\mathbf{C}) - j - 1.$$

We have by the lemma 2.15 for $j < \mathbf{Ht}(\mathbf{C})$, $\mathbf{C}^{(2j+1)} \subset \mathbf{C}^{(2j+3)}$, then

$$d(\mathbf{C}^{(2j+3)}) \leq d(\mathbf{C}^{(2j+1)}) - 1.$$

But,

$$d(\mathbf{C}^{(2j+1)}) \leq d(\mathbf{C}) - j.$$

Then,

$$d(\mathbf{C}^{(2j+3)}) \leq d(\mathbf{C}) - (j+1).$$

Hence the result. $\square$

Corollary 2.22. $\forall\, j \geq \boldsymbol{Ht}(\mathbf{C})$, $d(\mathbf{C}^{(2j+1)}) \leq d(\mathbf{C}) - \boldsymbol{Ht}(\mathbf{C})$.

Proposition 2.23. *Let* $\mathbf{C}$ *be an* $[n,k,d]_q$ *linear code over* $GF(q)$, *and let* $Q(M)H$ *be a parity check matrix of the code* $P(\mathbf{C})$ *where* $Q(M) = a_1 I_r + a_3 M + \cdots + a_{2\nu+1} M^\nu$ *and* $M = HH^T$. *Then*

$$P(\mathbf{C}) = \mathbf{C} \Longleftrightarrow Q(M) \text{ is invertible}.$$

Proof. Let $x \in P(\mathbf{C})$, then $x(Q(M)H)^T = xH^TQ(M) = 0$.
$Q(M)$ is invertible implies $xH^T = 0$, hence $x \in \mathbf{C}$. Thus $P(\mathbf{C}) = \mathbf{C}$.
Conversely, we assume that $P(\mathbf{C}) = \mathbf{C}$ and $Q(M)$ is not invertible. Then we have $rank(Q(M)) < n - k$ ($Q(M)$ is not a full rank matrix), thus $rank(Q(M)H) \leq min(rank(Q(M)), rank(H)) = rank(Q(M))$.
Consequently, $dim(P(\mathbf{C})) = n - rank(Q(M)H) > k$. Absurd as $dim(\mathbf{C}) = k$. □

Proposition 2.24. *Let $\mathbf{C}$ be an $[n, k, d]_q$ linear code over $GF(q)$, then the syndrome $S(x)$ of $x \in GF(q)^n$ with respect to $P(\mathbf{C})$ is*

$$S_{P(\mathbf{C})}(x) = Q(M)S_{\mathbf{C}}(x),$$

where $S_{\mathbf{C}}(x)$ is the syndrome of x with respect to $\mathbf{C}$.

Proof. We recall that the syndrome of x is defined by $S_{\mathbf{C}}(x) = Hx^T$ [7].
Let $x \in GF(q)^n$, then we have

$$\begin{aligned} S_{P(\mathbf{C})}(x) &= Q(M)Hx^T \\ &= Q(M)S_{\mathbf{C}}(x). \end{aligned}$$

□

Corollary 2.25. *If $P(\mathbf{C}) = \mathbf{C}^{(2j+1)}$, then for $j \in \mathbb{N}$*

$$S_{\mathbf{C}^{(2j+1)}}(x) = M^jS_{\mathbf{C}}(x).$$

The following algorithm represents the syndrome decoding corresponding to the code $P(\mathbf{C})$.

Algorithm 2.26.
If we already know the syndrome decoding by the code $\mathbf{C}$, then for a received word x we proceed as follows :
Step 1: We calculate its syndrome $S_{P(\mathbf{C})}(x) = Q(M)S_{\mathbf{C}}(x)$. Hence two cases are discussed. If $Q(M)$ is invertible, then the coset leaders will not change and we find the same syndromes corresponding to $\mathbf{C}$ with a permutation. If $Q(M)$ is not invertible, then since $dim(P(\mathbf{C})) > dim(\mathbf{C})$ we have the number of cosets founded by $P(\mathbf{C})$ is smaller than the number of cosets corresponds to $\mathbf{C}$, this means that there are syndromes that will be repeated. Since error patterns $\mathbf{e}$ verify $w(\mathbf{e}) \leq \lfloor \dfrac{d(\mathbf{C}) - 1}{2} \rfloor$ and $d(P(\mathbf{C})) \leq d(\mathbf{C})$, then also the number of coset leaders will decrease.

Step 2: We redress the syndrome table by multiplying all cosets by $Q(M)$ and after elimination of repeating cosets we find the coset leader u next to the syndrome $S_{P(\mathbf{C})}(x) = S_{P(\mathbf{C})}(u)$ in the syndrome table.

Step 3: We decode x as $y = x - u$.

The following examples are generated by the computer algebra system SAGE.

Example 2.27. In this example, we take the case of random codes. As we can see, the code remains stable if we use an odd polynomial $P(X)$ such that $Q(M)$ is invertible. However, if $Q(M)$ is not invertible, the dimension increases and the minimum distance decreases while the length always stays the same.

TABLE 1. Some examples with random codes

q	(n,k,d) *of* $\mathbf{C}$	$P(X)$	*is* $Q(M)$ *invertible ?*	(n,k,d) *of* $P(\mathbf{C})$
4	$(10,4,4)$	$X^{11}+X^9+X$	*yes*	$(10,4,4)$
4	$(15,7,5)$	$X^{19}+X^{13}+1$	*yes*	$(15,7,5)$
2	$(24,12,4)$	X^7+X^5+X	*yes*	$(24,12,4)$
32	$(8,5,3)$	$X^9+X^5+X^3$	*yes*	$(8,5,3)$
16	$(10,3,7)$	X^7+X^5+X	*no*	$(10,7,3)$
8	$(17,8,7)$	X^5+X	*no*	$(17,9,5)$
8	$(15,6,6)$	$X^{11}+X^7$	*no*	$(15,9,4)$
8	$(20,8,8)$	X^7+X^5+X	*no*	$(20,9,6)$

Example 2.28. In this example, we take the case of known code classes for example rational Goppa codes [1, 5], with the polynomial $Q(X)$ given directly. The dimension always increases while the minimum distance decreases. In the first case of the cyclic code, since the matrix $M = HH^T$ is zero, we find the ambient space for any chosen $Q(X)$. We also note that the parameters of the new code found depend on the polynomial chosen. There is no clear relationship between these parameters and the degree of the polynomial, this dependency is mysterious.

TABLE 2. Some examples with known codes

q	*Type of the code*	(n,k,d) *of* $\mathbf{C}$	$Q(X)$	(n,k,d) *of* $P(\mathbf{C})$
8	*Cyclic code*	$(7,4,3)$	*any* $Q(X)$	$GF(8)^7=(7,7,1)$
2	*BCH code*	$(15,5,7)$	X^4+X^2	$(15,11,1)$
2	*BCH code*	$(15,7,4)$	X	$(15,11,2)$
2	*BCH code*	$(15,7,4)$	X^2	$(15,13,1)$
2	*BCH code*	$(15,7,4)$	X^3+X^2+X+1	$(15,9,3)$
8	*Reed − Solomon code*	$(7,2,6)$	X^7+X^5+1	$(7,4,4)$
8	*Reed − Solomon code*	$(7,2,6)$	X	$(7,3,1)$
11	*Reed − Solomon code*	$(10,5,6)$	$X+1$	$(10,6,5)$
64	*Rational Goppa code*	$(55,16,19)$	X^7+X	$(55,31,1)$
8	*Rational Goppa code*	$(8,2,5)$	X^2+X+1	$(8,4,1)$
2	*Kasami code*	$(16,9,4)$	X^7+X	$(16,14,1)$

Remark 2.29. If we take a non-trivial cyclic code $\mathbf{C}$ and a polynomial $P(X)$ with the same above conditions, then the code $P(\mathbf{C})$ is not necessary cyclic.

Example 2.30. We consider over $GF(2)$ the example of the $[15, 5, 7]$ BCH code $\mathbf{C}$ which is cyclic with the generator polynomial $g(x) = X^{10} + X^8 + X^5 + X^4 + X^2 + X + 1$ and we take $P(X) = X^9 + X^5 \in GF(2)[X]$. Then the code $P(\mathbf{C})$ with parameters $[15, 11, 1]$ is not cyclic since $c = (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \in P(\mathbf{C})$ and $c' = (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$ is not a codeword in $P(\mathbf{C})$.

Example 2.31. Here we study the height of some linear codes. We note that sometimes the minimum distance decreases rapidly towards its stability (respectively the dimension increases rapidly), the case of rational Goppa code with $q = 64$ shows that. For some codes, the height is 0 i.e. the code is stable by default. Moreover, when the height is 1, there are in fact two possibilities: either the initial code will give a code strictly included in the whole space, or will give the ambient space such the case of Reed-Solomon codes below.

Table 3. Height of some codes

q	*Type of the code*	(n, k, d) *of* $\mathbf{C}$	$\mathbf{Ht}(\mathbf{C})$	(n, k, d) *of* $\mathbf{C}^{(2\mathbf{Ht}(\mathbf{C})+1)}$
2	*BCH code*	$(31, 11, 11)$	1	$(31, 21, 4)$
2	*BCH code*	$(15, 7, 4)$	2	$(15, 13, 1)$
2	*BCH code*	$(15, 5, 7)$	2	$(15, 11, 1)$
59	*Reed – Solomon code*	$(40, 12, 29)$	0	$(40, 12, 29)$
7	*Reed – Solomon code*	$(7, 5, 3)$	1	$(7, 7, 1)$
8	*Reed – Solomon code*	$(7, 2, 6)$	1	$(7, 3, 1)$
8	*Reed – Solomon code*	$(10, 5, 6)$	1	$(10, 10, 1)$
8	*Rational Goppa code*	$(8, 2, 5)$	1	$(8, 4, 2)$
32	*Rational Goppa code*	$(27, 2, 11)$	3	$(27, 5, 9)$
64	*Rational Goppa code*	$(55, 16, 19)$	1	$(55, 31, 1)$
2	*Golay code*	$(24, 12, 8)$	1	$(24, 24, 1)$

2.2. **Spectral Theory.**

In this section, we introduce the notion of spectral theory, which manipulates the eigenvalues of the matrices constructed by the adjacency matrices of a Tanner graph presented below, in order to derive spectral links to give a lower bound on the minimum distance of the power of the initial code.

In the following proposition we show the relation between the eigenvalues of the matrix $H^T H$ and those of the matrix $(Q(M)H)^T Q(M)H$, with $Q(X) \in GF(q)[X]$ is the same polynomial previously defined.

Proposition 2.32. *If x is an eigenvector of $H^T H$ associated with the eigenvalue μ, then x is an eigenvector of $(Q(M)H)^T Q(M)H$ associated with the eigenvalue $\mu Q(\mu)^2$, where $Q(M) = a_1 I_r + a_3 M + \cdots + a_{2\nu+1} M^\nu$ and $M = HH^T$.*

Proof. Let μ be an eigenvalue of the matrix $H^T H$ associated with the eigenvector x, then

$$\begin{aligned} H^T Hx &= \mu x \\ HH^T Hx &= \mu Hx. \end{aligned}$$

Since $M = HH^T$, then

$$\begin{aligned} MHx &= \mu Hx \\ M^2 Hx &= \mu MHx = \mu^2 Hx \\ M^3 Hx &= \mu^2 MHx = \mu^3 Hx \\ &\vdots \\ M^\nu Hx &= \mu^\nu Hx. \end{aligned}$$

We multiply each equality by a coefficient to obtain the polynomial Q applied to M and μ after term-by-term summation.
Explicitly we find

$$Q(M)Hx = Q(\mu)Hx,$$

where $Q(M) = a_1 I_r + a_3 M + \cdots + a_{2\nu+1} M^\nu$.
This is equivalent to

$$\begin{aligned} H^T Q(M)Q(M)Hx &= H^T Q(M)Q(\mu)Hx \\ &= Q(\mu)H^T Q(M)Hx \\ &= Q(\mu)H^T Q(\mu)Hx \\ &= Q(\mu)^2 H^T Hx \\ &= \mu Q(\mu)^2 x. \end{aligned}$$

□

Remark 2.33. The result of the proposition (2.32) is valid if H and Q are defined over any field.

In the following proposition for a matrix H defined over any field, we show the relation between the eigenvalues of the matrix $H^T H$ and those of the matrix $(M^\nu H)^T M^\nu H$ with $M = HH^T$ for a certain nonnegative integer ν.

Proposition 2.34. *If $H^T H$ is diagonalizable with eigenvalues $\mu_1, \mu_2, \cdots, \mu_s$ counted with their multiplicities. Then $\forall \nu \in \mathbb{N}$, $(M^\nu H)^T M^\nu H$ is diagonalizable with eigenvalues $\mu_1^{2\nu+1}, \mu_2^{2\nu+1}, \cdots, \mu_s^{2\nu+1}$ counted with their multiplicities.*

Proof. Since $H^T H$ is diagonalizable, then it is similar to a diagonal matrix D which contains on its diagonal all the eigenvalues of the matrix $H^T H$, i.e. there exists an invertible matrix P such that $H^T H = PDP^{-1}$.

This means that $\forall \nu \in \mathbb{N}$, $(H^T H)^{2\nu+1} = PD^{2\nu+1}P^{-1}$.
On the other hand we have,

$$\begin{aligned}(H^T H)^{2\nu+1} &= (H^T H)^{\nu}(H^T H)^{\nu} H^T H \\ &= H^T (HH^T)^{\nu}(HH^T)^{\nu} H \\ &= H^T M^{\nu} M^{\nu} H \\ &= (M^{\nu} H)^T M^{\nu} H.\end{aligned}$$

Therefore, $(M^{\nu}H)^T M^{\nu} H = PD^{2\nu+1}P^{-1}$. Consequently, the desired result. □

In the following, we restrict our study to the case of a Tanner graph Γ, with the $(n+r)\times(n+r)$ real-valued adjacency matrix

$$A = \begin{bmatrix} 0 & H \\ H^T & 0 \end{bmatrix}. \tag{2.5}$$

Note that the matrix $H^T H$ is a real symmetric matrix then it is diagonalizable with $\mu_1 > \mu_2 > \cdots > \mu_s$ are its ordered distinct eigenvalues [9].
From the proposition (2.34), we have the following corollary.

Corollary 2.35. *Let $\mu_1 > \mu_2 > \cdots > \mu_s$ be the ordered distinct eigenvalues of $H^T H$, then for a certain nonnegative integer ν, $\mu_1^{2\nu+1} > \mu_2^{2\nu+1} > \cdots > \mu_s^{2\nu+1}$ are the ordered distinct eigenvalues of $(M^{\nu}H)^T M^{\nu} H$.*

The aim of the following theorem is to find a lower bound on the minimum distance of the code $\mathbf{C}^{(2\nu+1)}$ based on the spectral study of the matrix $(M^{\nu}H)^T M^{\nu} H$ constructed from the adjacency matrix A (2.5) of a Tanner graph Γ by calculating A^{ν} for a certain nonnegative integer ν. Then according to the Theorem 3.1 (page 3 presented in [9]). We have

Theorem 2.36. *If Γ is a regular connected graph with adjacency matrix A, and n bit nodes of uniform degree m, and $r = n-k$ parity nodes of uniform degree j, then the minimum distance of the code $\mathbf{C}^{(2\nu+1)}$ satisfies*

$$d(\mathbf{C}^{(2\nu+1)}) \geq \frac{n(2m(mj)^{\nu} - \mu_2^{2\nu+1})}{(mj)^{2\nu+1} - \mu_2^{2\nu+1}},$$

where $0 \leq \nu \leq \boldsymbol{Ht}(\mathbf{C})$.

Proof. Let $\mathbf{C}$ be a linear code with the parity check matrix H constructed from a Tanner graph with the adjacency matrix A (2.5). For $0 \leq \nu \leq \mathbf{Ht}(\mathbf{C})$, let $\mathbf{C}^{(2\nu+1)}$ be the linear code with the parity check matrix $M^{\nu}H$ such that $M = HH^T$. The minimum distance of $\mathbf{C}^{(2\nu+1)}$ is denoted by D.
Let x be a real-valued vector of length n that represents a codeword with the minimum weight, with a one at each position where the minimum weight codeword is non-zero and zeros elsewhere. Since Γ is regular and connected, then the first and unique eigenvector of $H^T H$ that can be taken is $e_1 = \dfrac{(1,1,...,1)^T}{\sqrt{n}}$ with $\mu_1 = mj$. Consequently and by the corollary (2.35), the first and unique eigenvector of $(M^{\nu}H)^T M^{\nu} H$ is e_1 with $\mu_1^{2\nu+1}$.

Let x_i be the projection of x onto the $i-th$ eigenspace of the matrix $(M^\nu H)^T M^\nu H$, we have

$$< x, x >= ||x||^2 = D.$$

Since $e_1 = \frac{(1, 1, ..., 1)^T}{\sqrt{n}}$, then

$$\begin{aligned}
x_1 &=< x, e_1 > e_1 \\
x_1 &=< x, \frac{(1, 1, ..., 1)^T}{\sqrt{n}} > e_1 \\
x_1 &= \frac{D}{\sqrt{n}} e_1.
\end{aligned}$$

Hence,

$$\begin{aligned}
< x_1, x_1 > &= \frac{D^2}{n} < e_1, e_1 > \\
||x_1||^2 &= \frac{D^2}{n} ||e_1||^2.
\end{aligned}$$

Since $||e_1||^2 = 1$, then $||x_1||^2 = \frac{D^2}{n}$.

Let $Hx = (a_0, a_1, ..., a_{r-1})$ with $a_i = \sum_{k=0}^{n-1} h_{ik} x_k$, and let $X = (HH^T)^\nu Hx$ with $X_i = ((HH^T)^\nu Hx)_i$ is the weight on the $i-th$ parity i.e. the weight corresponding to the $i-th$ vector position X_i, where $0 \leq i \leq r-1$.

We have for $0 \leq \nu \leq \mathbf{Ht}(\mathbf{C})$,

$$||(HH^T)^\nu Hx||^2 = \sum_{i=0}^{r-1} X_i^2 \geq 2 \sum_{i=0}^{r-1} X_i = 2m(mj)^\nu D.$$

Where the inequality follows from each X_i being greater than 2. This depends on the choice of the real-valued vector x and the distribution of its elements.

To understand the idea, we will explain what happened in the case of $\nu = 1$. The rest is technical, by increasing power. We put now for $0 \leq s \leq r-1$,

$$X'_s = (HH^T Hx)_s = \sum_{k=0}^{r-1} HH^T_{sk} a_k.$$

Hence, as $(HH^T)_{ij} = \sum_{k=0}^{n-1} h_{ik}h_{jk}$ for $0 \leq i, j \leq r-1$, we have

$$\begin{aligned}
\sum_{s=0}^{r-1} X'_s &= \sum_{s=0}^{r-1}\sum_{k=0}^{r-1} HH^T_{sk}a_k \\
&= \sum_{k=0}^{r-1} HH^T_{0k}a_k + \sum_{k=0}^{r-1} HH^T_{1k}a_k + \cdots + \sum_{k=0}^{r-1} HH^T_{r-1k}a_k \\
&= \sum_{k=0}^{r-1}(\sum_{s=0}^{r-1} HH^T_{sk})a_k.
\end{aligned}$$

Since each column of H has m ones and each row j ones, hence the sum of all elements in any column of HH^T is mj. In fact, by taking the $k-th$ column of HH^T, we have $HH^T_{sk} = \sum_{p=0}^{n-1} h_{sp}h_{kp}$, hence

$$\begin{aligned}
\sum_{s=0}^{r-1} HH^T_{sk} &= \sum_{p=0}^{n-1} h_{kp}(\sum_{s=0}^{r-1} h_{sp}) \\
&= m\sum_{p=0}^{n-1} h_{kp} \\
&= mj.
\end{aligned}$$

Consequently, $\sum_{s=0}^{r-1} X'_s = mj\sum_{k=0}^{r-1} a_k = m^2jD$. Indeed,

$$\begin{aligned}
\sum_{k=0}^{r-1} a_k &= \sum_{k=0}^{r-1}\sum_{p=0}^{n-1} h_{kp}x_p \\
&= \sum_{p=0}^{n-1} x_p(\sum_{k=0}^{r-1} h_{kp}) \\
&= m\sum_{p=0}^{n-1} x_p \\
&= mD.
\end{aligned}$$

Then by repeating this process for $0 \leq \nu \leq \mathbf{Ht}(\mathbf{C})$, the key idea is to sum the components of a fixed column of the matrix $(HH^T)^\nu$ which is exactly $(mj)^\nu$, to have clearly

$$\sum_{i=0}^{r-1} X_i = m(mj)^\nu D.$$

Now by converting this to eigenspace representation,

$$\begin{aligned}||(HH^T)^\nu Hx||^2 &= \sum_{i=1}^{s}\mu_i^{2\nu+1}||x_i||^2 = \mu_1^{2\nu+1}\frac{D^2}{n} + \sum_{i=2}^{s}\mu_i^{2\nu+1}||x_i||^2 \\ &\leq \mu_1^{2\nu+1}\frac{D^2}{n} + \mu_2^{2\nu+1}\sum_{i=2}^{s}||x_i||^2 = \mu_1^{2\nu+1}\frac{D^2}{n} + \mu_2^{2\nu+1}(||x||^2 - ||x_1||^2)\end{aligned}$$

Substituting from above,

$$\mu_1^{2\nu+1}\frac{D^2}{n} + \mu_2^{2\nu+1}(D - \frac{D^2}{n}) \geq 2m(mj)^\nu D.$$

Consequently, since $\mu_1 = mj$ we have,

$$d(\mathbf{C}^{(2\nu+1)}) = D \geq \frac{n(2m(mj)^\nu - \mu_2^{2\nu+1})}{(mj)^{2\nu+1} - \mu_2^{2\nu+1}}.$$

□

Remark 2.37. If we replace ν by 0 in the previous inequality, we arrive at the formula given by Tanner [9].

Example 2.38. We take the same example as in [9] of the $[7, 3, 4]$ expurgated Hamming code with the $i-th$ rows of the matrix H are the coefficients of the polynomial $\alpha^i(1 + \alpha^2 + \alpha^3) \mod (\alpha^7 + 1)$, for $0 \leq i \leq 6$. We have the matrix H^TH has as eigenvalues $\mu_1 = 9$ and $\mu_2 = 2$, with $m = 3$. Thus $d(\mathbf{C}) \geq 4$.
If we consider the code $\mathbf{C}^{(3)}$, then

$$d(\mathbf{C}^{(3)}) \geq \frac{7(2 \times 3 \times 9 - 2^3)}{9^3 - 2^3} \approx 0.44.$$

This bound is trivial since already the true minimum distance of $\mathbf{C}^{(3)}$ is 1.

Remark 2.39. To see the use of this result, and as the previous example shows, it is necessary to choose codes with large lengths and obviously others having a large minimum distance, since according to the simulations we observe that a lot of times the minimum distance decreases rapidly.

In the following proposition we give an upper bound on the height of the initial code $\mathbf{C}$.

Proposition 2.40. *Keeping all the previous notions, If $\mu_2^2 > \mu_1$, then the height r of the code $\mathbf{C}$ satisfies*

$$r \leq ln(\frac{2nm - \mu_1}{n-1})\frac{1}{ln(\frac{\mu_2^2}{\mu_1})}.$$

Proof. According to the theorem (2.36), we have for $\nu = r$,

$$n(2m(mj)^r - \mu_2^{2r+1}) \geq (mj)^{2r+1} - \mu_2^{2r+1}.$$

Hence,

$$\mu_1^r(2nm - \mu_1^{r+1}) \geq \mu_2^{2r+1}(n-1).$$

Then,

$$2nm - \mu_1^{r+1} \geq \mu_2(\frac{\mu_2^2}{\mu_1})^r(n-1).$$

As $\mu_1^{r+1} \geq \mu_1$, we have

$$2nm - \mu_1 \geq \mu_2(\frac{\mu_2^2}{\mu_1})^r(n-1).$$

In addition we have $\mu_2 > 1$ and $2nm - \mu_1 > n-1$. In fact,
$\mu_2^2 > \mu_1 = mj$ implies $\mu_2 > 1$ since $mj > 1$. And since $n > j$, we have $2n - j > n$ implies $m(2n-j) > mn > n-1$ i.e. $2mn - \mu_1 > n-1$.
Therefore,

$$\frac{2nm - \mu_1}{n-1} \geq (\frac{\mu_2^2}{\mu_1})^r.$$

Consequently,

$$r \leq ln(\frac{2nm - \mu_1}{n-1})\frac{1}{ln(\frac{\mu_2^2}{\mu_1})}.$$

□

Example 2.41. If we take the same first example in [8], for the $[9,2,3]$-regular LDPC code $\mathbf{C}$ with $\mu_1 = 6$, $\mu_2 = 3$ and $m = 2$. Since $\mu_2^2 > \mu_1$. Then

$$\begin{aligned} &r \leq ln(\frac{2 \times 9 \times 2 - 6}{9-1})\frac{1}{ln(\frac{9}{6})} \approx 3.25 \\ &r \leq 3. \end{aligned}$$

3. Conclusion

In this paper, we have given on the one hand a definition of an odd polynomial applied to a linear code, based on the correspondence between the theory of error-correcting codes and that of graph theory. This investigation has enabled us to extract a new notion called the height which characterizes a linear code. We generated many examples and gave results on the parameters of the new code obtained. On the other hand, based on the spectral study links we gave a lower bound on the minimum distance of the code power given by the Tanner graph. An upper bound on the height is then given. As perspectives behind this work, we think about the decoding problem i.e. finding an efficient decoder of the code $P(\mathbf{C})$ if we first know a decoder of $\mathbf{C}$.

Acknowledgement. The first author thanks CNRST for its support under the « PhD-Associate Scholarship - PASS » program.
The third author was supported by "Ministère de l'Enseignement supérieur, de la Recherche scientifique et de l'Innovation". Morocco.

References

1. Abdelmoumen, K., Ben-Azza, H., & Otmani, A. (2016). Pade approximants and key lattices for decoding alternant codes. Gulf Journal of Mathematics, 4(4). https://doi.org/10.56947/gjom.v4i4.278
2. Bondy, J. A., & Murty, U. S. R. (1976). Graph theory with applications (Vol. 290). London: Macmillan. https://doi.org/10.1137/1021086
3. Brouwer, A. E., & Haemers, W. H. (2011). Spectra of graphs. Springer Science & Business Media. https://doi.org/10.1007/978-1-4614-1939-6
4. Cvetković, D. M., Doob, M., & Sachs, H. (1980). Spectra of graphs: Theory and application. Academic Press.
5. Huffman, W. C., Kim, J. L., & Solé, P. (2021). Concise encyclopedia of coding theory. Chapman and Hall/CRC. https://doi.org/10.1201/9781315147901
6. Ling, S., & Xing, C. (2004). Coding theory: a first course. Cambridge university press. https://doi.org/10.1017/CBO9780511755279
7. MacWilliams, F. J., & Sloane, N. J. A. (1977). The theory of error-correcting codes (Vol. 16). Elsevier. https://doi.org/10.1016/S0924-6509(08)70523-3
8. Shin, M. H., Kim, J. S., & Song, H. Y. (2005). Generalization of Tanner's minimum distance bounds for LDPC codes. IEEE communications letters, 9(3), 240-242. https://doi.org/10.1109/LCOMM.2005.03002
9. Tanner, R. M. (2001). Minimum-distance bounds by graph analysis. IEEE Transactions on Information Theory, 47(2), 808-821. https://doi.org/10.1109/18.910591
10. Wicker, S. B., & Kim, S. (2002). Fundamentals of codes, graphs, and iterative decoding (Vol. 714). Springer Science & Business Media. https://doi.org/10.1007/b101872

[1] Sidi Mohammed Ben Abdellah University, École Normale Supérieure, Fez, Morocco

Email address: saber.darmoun@usmba.ac.ma

[2] Sidi Mohammed Ben Abdellah University, École Normale Supérieure, Fez, Morocco

Email address: khalid.abdelmoumen@usmba.ac.ma

[3] Moulay Ismail University, École Nationale Supérieure d'Arts et Métiers, Meknes, Morocco

Email address: h.benazza@umi.ac.ma