Exploration of AWGNC and BSC Pseudocodeword Redundancy

Jens Zumbrägel, Mark F. Flanagan, and Vitaly Skachek

Abstract— The AWGNC, BSC, and max-fractional *pseudocodeword redundancy* $\rho(\mathcal{C})$ of a code $\mathcal{C}$ is defined as the smallest number of rows in a parity-check matrix such that the corresponding minimum pseudoweight is equal to the minimum Hamming distance of $\mathcal{C}$. This paper provides new results on the AWGNC, BSC, and max-fractional pseudocodeword redundancies of codes. The pseudocodeword redundancies for all codes of small length (at most 9) are computed. Also, comprehensive results are provided on the cases of cyclic codes of length at most 250 for which the eigenvalue bound of Vontobel and Koetter is sharp.

I. Introduction

Pseudocodewords play a significant role in the finite-length analysis of binary linear low-density parity-check (LDPC) codes under linear-programming (LP) or message-passing (MP) decoding (see e.g. [1], [2]). The concept of *pseudoweight* of a pseudocodeword was introduced in [3] as an analog to the pertinent parameter in the maximum likelihood (ML) decoding scenario, i.e. the signal Euclidean distance in the case of the additive white Gaussian noise channel (AWGNC), or the Hamming distance in the case of the binary symmetric channel (BSC). Accordingly, for a binary linear code $\mathcal{C}$ and a parity-check matrix $\boldsymbol{H}$ of $\mathcal{C}$, the (AWGNC or BSC) minimum pseudoweight $\mathrm{w}^{\min}(\boldsymbol{H})$ may be considered as a first-order measure of decoder error-correcting performance for LP or MP decoding. Note that $\mathrm{w}^{\min}(\boldsymbol{H})$ may be different for different matrices $\boldsymbol{H}$: adding redundant rows to $\boldsymbol{H}$ introduces additional constraints on the so-called *fundamental cone* and may thus increase the minimum pseudoweight. Another closely related measure is the max-fractional weight (pseudoweight). It serves as a lower bound on both AWGNC and BSC pseudoweights.

The AWGNC (or BSC) pseudocodeword redundancy $\rho_{\mathrm{AWGNC}}(\mathcal{C})$ (or $\rho_{\mathrm{BSC}}(\mathcal{C})$, respectively) of a code $\mathcal{C}$ is defined as the minimum number of rows in a parity-check matrix $\boldsymbol{H}$ such that the corresponding minimum pseudoweight $\mathrm{w}^{\min}(\boldsymbol{H})$ is as large as its minimum Hamming distance d. It is set to infinity if there is no such matrix. We sometimes simply write $\rho(\mathcal{C})$, when the type of the channel is clear from the context.

J. Zumbrägel and M.F. Flanagan are with the Claude Shannon Institute, University College Dublin, Belfield, Dublin 4, Ireland. Emails: `jens.zumbragel@ucd.ie`, `mark.flanagan@ieee.org`.

V. Skachek is with Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, 637371 Singapore. Email: `vitaly.skachek@ntu.edu.sg`.

The pseudocodeword redundancy for the binary erasure channel (BEC), $\rho_{\mathrm{BEC}}(\mathcal{C})$, was studied in [4], where it was shown to be finite for any binary linear code $\mathcal{C}$. The authors also presented some bounds on $\rho_{\mathrm{BEC}}(\mathcal{C})$ for general linear codes, and for some specific families of codes. The study of BSC pseudoredundancy was initiated in [5], where the authors presented bounds on $\rho_{\mathrm{BSC}}(\mathcal{C})$ for various families of codes. In a recent work [6], we provided some bounds on $\rho_{\mathrm{AWGNC}}(\mathcal{C})$ and $\rho_{\mathrm{BSC}}(\mathcal{C})$ for general linear codes. In particular, [6] listed some preliminary results regarding the AWGNC and BSC pseudocodeword redundancies of short codes; this paper provides more comprehensive results in this direction.

The outline of the paper is as follows. After providing detailed definitions in Section II we prove several new theoretical results on the pseudocodeword redundancy in Sections III and IV. The next two sections are devoted to experimental results; Section V examines the pseudocodeword redundancy for all codes of small length, and Section VI deals with cyclic codes that meet the eigenvalue bound of Vontobel and Koetter.

II. General Settings

Let $\mathcal{C}$ be a code of length $n \in \mathbb{N}$ over the binary field $\mathbb{F}_2$, defined by

$$\mathcal{C} = \ker \boldsymbol{H} = \{\boldsymbol{c} \in \mathbb{F}_2^n \ : \ \boldsymbol{H}\boldsymbol{c}^T = \boldsymbol{0}^T\} \tag{1}$$

where $\boldsymbol{H}$ is an $m \times n$ *parity-check matrix* of the code $\mathcal{C}$. Obviously, the code $\mathcal{C}$ may admit more than one parity-check matrix, and all the codewords form a linear vector space of dimension $k \geq n - m$. We say that k is the *dimension* of the code $\mathcal{C}$. We denote by $d(\mathcal{C})$ (or just d) the minimum Hamming distance (also called the minimum distance) of $\mathcal{C}$. The code $\mathcal{C}$ may then be referred to as an $[n, k, d]$ linear code over $\mathbb{F}_2$.

The parity-check matrix $\boldsymbol{H}$ is said to be (w_c, w_r)-regular if every column of $\boldsymbol{H}$ has exactly w_c nonzero symbols, and every row of it has exactly w_r nonzeros. The matrix $\boldsymbol{H}$ is called w-regular if every row and every column in it has w nonzeros.

Denote the set of column indices and the set of row indices of $\boldsymbol{H}$ by $\mathcal{I} = \{1, 2, \ldots, n\}$ and $\mathcal{J} = \{1, 2, \ldots, m\}$, respectively. For $j \in \mathcal{J}$, we denote $\mathcal{I}_j \triangleq \{i \in \mathcal{I} \ : \ H_{j,i} \neq 0\}$, and for $i \in \mathcal{I}$, we denote $\mathcal{J}_i \triangleq \{j \in \mathcal{J} \ : \ H_{j,i} \neq 0\}$. The *fundamental cone* of $\boldsymbol{H}$, denoted $\mathcal{K}(\boldsymbol{H})$, is defined in [7] and [2] as the set of vectors $\boldsymbol{x} \in \mathbb{R}^n$ that satisfy

$$\forall j \in \mathcal{J}, \ \forall \ell \in \mathcal{I}_j \ : \ x_\ell \leq \sum_{i \in \mathcal{I}_j \setminus \{\ell\}} x_i \,, \tag{2}$$

$$\forall i \in \mathcal{I} \ : \ x_i \geq 0 \,. \tag{3}$$

The vectors $\boldsymbol{x} \in \mathbb{R}^n$ satisfying (2) and (3) are called *pseudocodewords* of $\mathcal{C}$ with respect to the parity-check matrix $\boldsymbol{H}$. Note that the fundamental cone $\mathcal{K}(\boldsymbol{H})$ depends on the parity-check matrix $\boldsymbol{H}$ rather than on the code $\mathcal{C}$ itself. At the same time, the fundamental cone is independent of the underlying communication channel.

The BEC, AWGNC, BSC pseudoweights and max-fractional weight of a nonzero pseudocodeword $\boldsymbol{x} \in \mathcal{K}(\boldsymbol{H})$ were defined in [3] and [2] as follows:

$$\mathsf{w}_{\text{BEC}}(\boldsymbol{x}) \triangleq |\text{supp}(\boldsymbol{x})| \ ,$$

$$\mathsf{w}_{\text{AWGNC}}(\boldsymbol{x}) \triangleq \frac{\left(\sum_{i \in \mathcal{I}} x_i\right)^2}{\sum_{i \in \mathcal{I}} x_i^2} \ .$$

Let $\boldsymbol{x}'$ be a vector in $\mathbb{R}^n$ with the same components as $\boldsymbol{x}$ but in non-increasing order. For $i-1 < \xi \leq i$, where $1 \leq i \leq n$, let $\phi(\xi) \triangleq x_i'$. Define $\Phi(\xi) \triangleq \int_0^\xi \phi(\xi')\, d\xi'$ and

$$\mathsf{w}_{\text{BSC}}(\boldsymbol{x}) \triangleq 2\, \Phi^{-1}(\Phi(n)/2) \ .$$

Finally, the max-fractional weight of $\boldsymbol{x}$ is defined as

$$\mathsf{w}_{\text{max-frac}}(\boldsymbol{x}) \triangleq \frac{\sum_{i \in \mathcal{I}} x_i}{\max_{i \in \mathcal{I}} x_i} \ .$$

We define the BEC *minimum pseudoweight* of the code $\mathcal{C}$ with respect to the parity-check matrix $\boldsymbol{H}$ as

$$\mathsf{w}_{\text{BEC}}^{\min}(\boldsymbol{H}) \triangleq \min_{\boldsymbol{x} \in \mathcal{K}(\boldsymbol{H}) \setminus \{\mathbf{0}\}} \mathsf{w}_{\text{BEC}}(\boldsymbol{x}) \ .$$

The quantities $\mathsf{w}_{\text{AWGNC}}^{\min}(\boldsymbol{H})$, $\mathsf{w}_{\text{BSC}}^{\min}(\boldsymbol{H})$ and $\mathsf{w}_{\text{max-frac}}^{\min}(\boldsymbol{H})$ are defined similarly. When the type of pseudoweight is clear from the context, we might use the notation $\mathsf{w}^{\min}(\boldsymbol{H})$. Note that all four minimum pseudoweights are upper bounded by d, the code's minimum distance.

Then we define the BEC *pseudocodeword redundancy* of the code $\mathcal{C}$ as

$$\rho_{\text{BEC}}(\mathcal{C}) \triangleq \inf\{\#\text{rows}(\boldsymbol{H}) \mid \ker \boldsymbol{H} = \mathcal{C}\,, \ \mathsf{w}_{\text{BEC}}^{\min}(\boldsymbol{H}) = d\} \ ,$$

where $\inf \varnothing \triangleq \infty$, and similarly we define the pseudocodeword redundancies $\rho_{\text{AWGNC}}(\mathcal{C})$, $\rho_{\text{BSC}}(\mathcal{C})$ and $\rho_{\text{max-frac}}(\mathcal{C})$ for the AWGNC and BSC pseudoweights, and the max-fractional weight. When the type of pseudocodeword redundancy is clear from the context, we might use the notation $\rho(\mathcal{C})$. We remark that all pseudocodeword redundancies satisfy $\rho(\mathcal{C}) \geq r \triangleq n - k$.

We describe the behavior of the pseudocodeword redundancy and the minimum pseudoweight for a given binary linear $[n, k, d]$ code $\mathcal{C}$ by introducing four classes of codes:

(class 0) $\rho(\mathcal{C})$ is infinite, i.e. there is no parity-check matrix $\boldsymbol{H}$ with $d = \mathsf{w}^{\min}(\boldsymbol{H})$,

(class 1) $\rho(\mathcal{C})$ is finite, but $\rho(\mathcal{C}) > r$,

(class 2) $\rho(\mathcal{C}) = r$, but $\mathcal{C}$ is not in class 3,

(class 3) $d = \mathsf{w}^{\min}(\boldsymbol{H})$ for *every* parity-check matrix $\boldsymbol{H}$ of $\mathcal{C}$.

III. Basic Results

The next lemma is taken from [2].

Lemma 3.1: Let $\mathcal{C}$ be a binary linear code with the parity-check matrix $\boldsymbol{H}$. Then,

$$\mathsf{w}_{\text{max-frac}}^{\min}(\boldsymbol{H}) \ \leq \ \mathsf{w}_{\text{AWGNC}}^{\min}(\boldsymbol{H}) \ \leq \ \mathsf{w}_{\text{BEC}}^{\min}(\boldsymbol{H}) \ ,$$
$$\mathsf{w}_{\text{max-frac}}^{\min}(\boldsymbol{H}) \ \leq \ \mathsf{w}_{\text{BSC}}^{\min}(\boldsymbol{H}) \ \leq \ \mathsf{w}_{\text{BEC}}^{\min}(\boldsymbol{H}) \ .$$

The following theorem is a straightforward corollary to Lemma 3.1.

Theorem 3.2: Let $\mathcal{C}$ be a binary linear code. Then,

$$\rho_{\text{max-frac}}(\mathcal{C}) \ \geq \ \rho_{\text{AWGNC}}(\mathcal{C}) \ \geq \ \rho_{\text{BEC}}(\mathcal{C}) \ ,$$
$$\rho_{\text{max-frac}}(\mathcal{C}) \ \geq \ \rho_{\text{BSC}}(\mathcal{C}) \ \geq \ \rho_{\text{BEC}}(\mathcal{C}) \ .$$

The following results hold with respect to the AWGNC and BSC pseudoweights, and the max-fractional weight.

Lemma 3.3: Let $\mathcal{C}$ be an $[n, k, d]$ code having t zero coordinates, and let $\mathcal{C}'$ be the $[n-t, k, d]$ code obtained by puncturing $\mathcal{C}$ at these coordinates. Then

$$\rho(\mathcal{C}') \leq \rho(\mathcal{C}) \leq \rho(\mathcal{C}') + t \ .$$

In the proof we use the following notation: We identify $\mathbb{R}^n$ with $\mathbb{R}^{\mathcal{I}}$, and for $x \in \mathbb{R}^{\mathcal{I}}$ and some subset $\mathcal{I}' \subseteq \mathcal{I}$ we let $\boldsymbol{x}|_{\mathcal{I}'} \in \mathbb{R}^{\mathcal{I}'}$ be the projection of $\boldsymbol{x}$ onto the coordinates in $\mathcal{I}'$.

Proof: Let $\mathcal{I}' \subseteq \mathcal{I}$ be the set of nonzero coordinates of the code $\mathcal{C}$. To prove the first inequality, let $\boldsymbol{H}$ be a $\rho \times n$ parity-check matrix for $\mathcal{C}$. Consider its $\rho \times (n-t)$ submatrix $\boldsymbol{H}'$ consisting of the columns corresponding to $\mathcal{I}'$. Then $\boldsymbol{H}'$ is a parity-check matrix for $\mathcal{C}'$, and

$$\mathcal{K}(\boldsymbol{H}') = \{\boldsymbol{x}|_{\mathcal{I}'} : \boldsymbol{x} \in \mathcal{K}(\boldsymbol{H}), \ \boldsymbol{x}|_{\mathcal{I} \setminus \mathcal{I}'} = \mathbf{0}\} \ .$$

Therefore, $\mathsf{w}^{\min}(\boldsymbol{H}') \geq \mathsf{w}^{\min}(\boldsymbol{H})$, and this proves $\rho(\mathcal{C}') \leq \rho(\mathcal{C})$.

For the second inequality, let $\boldsymbol{H}'$ be a $\rho' \times (n-t)$ parity-check matrix for $\mathcal{C}'$. Now we consider a $(\rho'+t) \times n$ matrix $\boldsymbol{H}$ with the following properties: The upper $\rho' \times n$ submatrix of $\boldsymbol{H}$ consists of the columns of $\boldsymbol{H}'$ at positions $\mathcal{I}'$ and of zero-columns at positions $\mathcal{I} \setminus \mathcal{I}'$, and the lower $t \times n$ submatrix consists of rows of weight 1 that have 1s at the positions $\mathcal{I} \setminus \mathcal{I}'$. Then $\mathcal{C} = \ker \boldsymbol{H}$ and

$$\mathcal{K}(\boldsymbol{H}) = \{\boldsymbol{x} \in \mathbb{R}^{\mathcal{I}} : \boldsymbol{x}|_{\mathcal{I}'} \in \mathcal{K}(\boldsymbol{H}'), \ \boldsymbol{x}|_{\mathcal{I} \setminus \mathcal{I}'} = \mathbf{0}\} \ .$$

Consequently, $\mathsf{w}^{\min}(\boldsymbol{H}) = \mathsf{w}^{\min}(\boldsymbol{H}')$, and this proves $\rho(\mathcal{C}) \leq \rho(\mathcal{C}') + t$. ∎

Lemma 3.4: Let $\mathcal{C}$ be a code of minimum distance $d \leq 2$. Then $d = \mathsf{w}^{\min}(\boldsymbol{H})$ for any parity-check matrix $\boldsymbol{H}$ of $\mathcal{C}$, i.e. $\mathcal{C}$ is in class 3 (for AWGNC and BSC pseudoweight, and for max-fractional weight).

Proof: By Lemma 3.1 it suffices to prove this lemma for the max-fractional weight $\mathsf{w} = \mathsf{w}_{\text{max-frac}}$. Since $\mathsf{w}(\boldsymbol{x}) \geq 1$ holds for all nonzero pseudocodewords, we always have $\mathsf{w}^{\min}(\boldsymbol{H}) \geq 1$, which proves the result in the case $d = 1$.

Let $d = 2$ and $\boldsymbol{H}$ be a parity-check matrix for $\mathcal{C}$. Let $\boldsymbol{x} \in \mathcal{K}(\boldsymbol{H})$ and let x_ℓ be the largest coordinate. Since $d = 2$ there is no zero column in $\boldsymbol{H}$ and thus there exists a row j with $\ell \in \mathcal{I}_j$. Then $x_\ell \leq \sum_{i \in \mathcal{I} \setminus \{\ell\}} x_i$, hence $2x_\ell \leq \sum_{i \in \mathcal{I}} x_i$, and thus $\mathsf{w}(\boldsymbol{x}) \geq 2$. It follows $\mathsf{w}^{\min}(\boldsymbol{H}) \geq 2$ and the lemma is proved. ∎

IV. PARITY-CHECK MATRICES WITH ROWS OF WEIGHT 2

The main result of this section appears in the following lemma.

Lemma 4.1: Let H be a parity-check matrix of C such that every row in H has weight 2. Then:

(a) There is an equivalence relation on the set $\mathcal{I}$ of column indices of H such that for a vector $x \in \mathbb{R}^n$ with non-negative coordinates we have $x \in \mathcal{K}(H)$ if and only if x has equal coordinates within each equivalence class.

(b) The minimum distance of C is equal to its minimum AWGNC and BSC pseudoweights and its max-fractional weight with respect to H, i.e. $d(C) = \mathsf{w}^{\min}(H)$.

Proof: For (a), define the required relation R as follows: For $i, i' \in \mathcal{I}$ let $(i, i') \in R$ if and only if $i = i'$ or there exists an integer $\ell \geq 1$, column indices $i = i_0, i_1, \ldots, i_{\ell-1}, i_\ell = i' \in \mathcal{I}$ and row indices $j_1, \ldots, j_l \in \mathcal{J}$ such that

$$\{i_0, i_1\} = \mathcal{I}_{j_1}, \{i_1, i_2\} = \mathcal{I}_{j_2}, \ldots, \{i_{\ell-1}, i_\ell\} = \mathcal{I}_{j_\ell}.$$

This is an equivalence relation, and it defines equivalence classes over $\mathcal{I}$. It is easy to check that inequalities (2) imply that $x \in \mathcal{K}(H)$ if and only if $x_i = x_{i'}$ for any $(i, i') \in R$.

In order to prove (b), we note that the minimum (AWGNC, BSC or max-fractional) pseudoweight is always bounded above by the minimum distance of C, so we only have to show that the minimum pseudoweight is bounded below by the minimum distance.

Let $\mathcal{S} = \{S_1, S_2, \ldots, S_t\}$ be the set of equivalence classes of R, and let $d_S = |S|$ for $S \in \mathcal{S}$. It is easy to see that the minimum distance of C is $d = \min_{S \in \mathcal{S}} d_S$ (since the minimum weight nonzero codeword of C has non-zeros in the coordinates corresponding to a set $S \in \mathcal{S}$ of minimal size and zeros everywhere else).

Now let $x \in \mathcal{K}(H)$. Since the coordinates x_i, $i \in \mathcal{I}$, depend only on the equivalence classes, we may use the notation x_S, $S \in \mathcal{S}$. Let x_T be the largest coordinate. Then:

$$\mathsf{w}_{\text{max-frac}}(x) = \frac{\sum_{i \in \mathcal{I}} x_i}{x_T} \geq \frac{\sum_{i \in T} x_i}{x_T} = |T| = d_T \geq d.$$

Therefore, $\mathsf{w}_{\text{max-frac}}^{\min}(H) \geq d$, and by using Lemma 3.1, we obtain that $\mathsf{w}_{\text{AWGNC}}^{\min}(H) \geq d$ and $\mathsf{w}_{\text{BSC}}^{\min}(H) \geq d$. ∎

The following proposition is a stronger version of Lemma 4.1.

Proposition 4.2: Let H be an $m \times n$ parity-check matrix of C, and assume that $m - 1$ first rows in H have weight 2. Denote by $\widehat{H}$ the $(m-1) \times n$ matrix consisting of these rows, consider the equivalence relation of Lemma 4.1 (a) with respect to $\widehat{H}$, and assume that $\mathcal{I}_m$ intersects each equivalence class in at most one element. Then, the minimum distance of C is equal to its minimum AWGNC and BSC pseudoweights and its max-fractional weight with respect to H, i.e. $d(C) = \mathsf{w}^{\min}(H)$.

Proof: Let $\mathcal{S}$ be the set of classes of the aforementioned equivalence relation on $\mathcal{I}$, and let $d_S = |S|$ for $S \in \mathcal{S}$. Let

$$\mathcal{S}' = \{S \in \mathcal{S} : |S \cap \mathcal{I}_m| = 1\}.$$

Also let $\mathcal{S}'' = \mathcal{S} \backslash \mathcal{S}'$, so that $S \cap \mathcal{I}_m = \varnothing$ for all $S \in \mathcal{S}''$.

Let $x \in \mathcal{K}(H) \backslash \{0\}$. As before, since the coordinates x_i, $i \in \mathcal{I}$, depend only on the equivalence classes, we may use the notation x_S, $S \in \mathcal{S}$. The fundamental polytope constraints (2) and (3) may then be written as $x_S \geq 0$ for all $S \in \mathcal{S}$ and

$$\forall R \in \mathcal{S}' : x_R \leq \sum_{S \in \mathcal{S}' \backslash \{R\}} x_S, \qquad (4)$$

respectively, and the max-fractional pseudoweight of $x \in \mathcal{K}(H) \backslash \{0\}$ is given by

$$\mathsf{w}_{\text{max-frac}}(x) = \frac{\sum_{S \in \mathcal{S}} d_S x_S}{\max_{S \in \mathcal{S}} x_S}. \qquad (5)$$

Suppose $x \in \mathcal{K}(H) \backslash \{0\}$ has minimal max-fractional pseudoweight. Let x_T be its largest coordinate. First note that if there exists $R \in \mathcal{S}'' \backslash \{T\}$ with $x_R > 0$, setting x_R to zero results in a new pseudocodeword with lower max-fractional pseudoweight, which contradicts the assumption that x achieves the minimum. Therefore $x_R = 0$ for all $R \in \mathcal{S}'' \backslash \{T\}$. We next consider two cases.

Case 1: $T \in \mathcal{S}''$. If there exists $R \in \mathcal{S}'$ with $x_R > 0$, setting all such x_R to zero results in a new pseudocodeword with lower max-fractional pseudoweight, which contradicts the minimality of the max-fractional pseudoweight of x. Therefore x_T is the only positive coordinate of x, and by (5) the max-fractional pseudoweight of x is d_T.

Case 2: $T \in \mathcal{S}'$. In this case $x_R = 0$ for all $R \in \mathcal{S}''$. From inequality (4) for $R = T$ we obtain

$$x_T \leq \sum_{S \in \mathcal{S}' \backslash \{T\}} x_S.$$

With $d_0 \triangleq \min_{S \in \mathcal{S}' \backslash \{T\}} d_S$ it follows that

$$d_0 x_T \leq \sum_{S \in \mathcal{S}' \backslash \{T\}} d_0 x_S \leq \sum_{S \in \mathcal{S}' \backslash \{T\}} d_S x_S.$$

Consequently,

$$(d_T + d_0) x_T \leq \sum_{S \in \mathcal{S}} d_S x_S,$$

and thus $\mathsf{w}_{\text{max-frac}}(x) \geq d_T + d_0$. We conclude that the minimum max-fractional pseudoweight is given by

$$\mathsf{w}_{\text{max-frac}}^{\min}(H) = \min \left\{ \min_{S, T \in \mathcal{S}', S \neq T} \{d_S + d_T\}, \min_{S \in \mathcal{S}''} \{d_S\} \right\}.$$

But this is easily seen to be equal to the minimum distance d of the code.

Finally, by using Lemma 3.1, we obtain that $\mathsf{w}_{\text{AWGNC}}^{\min}(H) = d$ and $\mathsf{w}_{\text{BSC}}^{\min}(H) = d$. ∎

Remark: Note that the requirement that all $i \in \mathcal{I}_m$ belong to the different equivalence classes of $\widehat{H}$ in Proposition 4.2 is necessary. Indeed, consider the matrix

$$H = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

One can see that there are two equivalence classes for $\widehat{\boldsymbol{H}}$: $S_1 = \{1, 2, 3\}$, $S_2 = \{4\}$. The minimum distance of the corresponding code $\mathcal{C}$ is 4 (since $(1, 1, 1, 1)$ is the only nonzero codeword). However, $\boldsymbol{x} = (1, 1, 1, 3) \in \mathcal{K}(\boldsymbol{H})$ is a pseudocodeword of max-fractional weight 2.

Corollary 4.3: Let $\mathcal{C}$ be a code of length n and dimension 2. Then $\rho(\mathcal{C}) = n - 2$, i.e. $\mathcal{C}$ is of class at least 2 (for AWGNC and BSC pseudoweight, and for max-fractional weight).

Proof: We consider two cases.

- *Case 1: $\mathcal{C}$ has no zero coordinates.*
  Let $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ be two linearly independent codewords of $\mathcal{C}$. Define the following subsets of $\mathcal{I}$:

$$
\begin{aligned}
S_1 &\triangleq \{i \in \mathcal{I} \; : \; i \in \operatorname{supp}(\boldsymbol{c}_1) \text{ and } i \notin \operatorname{supp}(\boldsymbol{c}_2)\} \\
S_2 &\triangleq \{i \in \mathcal{I} \; : \; i \notin \operatorname{supp}(\boldsymbol{c}_1) \text{ and } i \in \operatorname{supp}(\boldsymbol{c}_2)\} \\
S_3 &\triangleq \{i \in \mathcal{I} \; : \; i \in \operatorname{supp}(\boldsymbol{c}_1) \text{ and } i \in \operatorname{supp}(\boldsymbol{c}_2)\}.
\end{aligned}
$$

  The sets S_1, S_2 and S_3 are pairwise disjoint. Since $\mathcal{C}$ has no zero coordinates, $\mathcal{I} = S_1 \cup S_2 \cup S_3$. The ordering of elements in $\mathcal{I}$ implies an ordering on the elements in each of S_1, S_2 and S_3. Assume that $S_1 = \{i_1, i_2, \cdots, i_{|S_1|}\}$ and $i_1 < i_2 < \cdots < i_{|S_1|}$. If $S_1 \neq \varnothing$, let $m_1 = i_1$ be the minimal element in S_1, and define an $(|S_1| - 1) \times n$ matrix H_1 as follows:

$$
(H_1)_{j,\ell} = \begin{cases} 1 & \text{if } i_j = \ell \text{ or } i_{j+1} = \ell \,, \\ & \qquad j = 1, 2, \cdots, |S_1| - 1 \,, \\ 0 & \text{otherwise} \,. \end{cases}
$$

  Similarly, define $(|S_2| - 1) \times n$ and $(|S_3| - 1) \times n$ matrices H_2 and H_3, with respect to S_2 and S_3. Let m_2 and m_3 be minimal elements of S_2 and S_3, respectively. Define also a $1 \times n$ matrix H_4:

$$
(H_4)_{1,\ell} = \begin{cases} 1 & \text{if } S_j \neq \varnothing \text{ and } m_j = \ell \\ & \qquad \text{for } j = 1, 2, 3 \,, \\ 0 & \text{otherwise} \,. \end{cases}
$$

  Finally, define an $(n - 2) \times n$ matrix $\boldsymbol{H}$ by $\boldsymbol{H}^T \triangleq [H_1^T \mid H_2^T \mid H_3^T \mid H_4^T]$. (Some of the S_i's might be equal to $\varnothing$, in which case the corresponding H_i is an $0 \times n$ "empty" matrix.) It is easy to see that all rows of $\boldsymbol{H}$ are linearly independent, and so it is of rank $n - 2$. It is also straightforward that for all $\boldsymbol{c} \in \mathcal{C}$ we have $\boldsymbol{c} \in \ker(\boldsymbol{H})$. Therefore, $\boldsymbol{H}$ is a parity-check matrix of $\mathcal{C}$.
  The matrix $\boldsymbol{H}$ has a form as in Proposition 4.2 (where S_1, S_2 and S_3 are corresponding equivalence classes over $\mathcal{I}$), and therefore $\rho(\mathcal{C}) = n - 2$.

- *Case 2: $\mathcal{C}$ has $t > 0$ zero coordinates.*
  Consider a code $\mathcal{C}'$ of length $n - t$ obtained by puncturing $\mathcal{C}$ in these t zero coordinates. From Case 1 (with respect to $\mathcal{C}'$), $\rho(\mathcal{C}') = n - t - 2$. By applying the rightmost inequality in Lemma 3.3, we have $\rho(C) \leq n - 2$. Since $k = 2$, we conclude that $\rho(C) = n - 2$. ∎

V. THE PSEUDOCODEWORD REDUNDANCY FOR CODES OF SMALL LENGTH

In this section we compute the AWGNC, BSC, and max-fractional pseudocodeword redundancies for all codes of small length. By Lemma 3.4 it is sufficient to examine only codes with minimum distance at least 3. Furthermore, in light of Lemma 3.3 we will consider only codes without zero coordinates, i.e. that have a dual distance of at least 2. Finally, we point out to Corollary 4.3 for codes of dimension 2, by which we may focus on codes with dimension at least 3.

A. The Algorithm

To compute the pseudocodeword redundancy of a code $\mathcal{C}$ we have to examine all possible parity-check matrices for the code $\mathcal{C}$, up to equivalence. Here, we say that two parity-check matrices $\boldsymbol{H}$ and $\boldsymbol{H}'$ for the code $\mathcal{C}$ are *equivalent* if $\boldsymbol{H}$ can be transformed into $\boldsymbol{H}'$ by a sequence of row and column permutations. In this case, $\mathrm{w}^{\min}(\boldsymbol{H}) = \mathrm{w}^{\min}(\boldsymbol{H}')$ holds for the AWGNC and BSC pseudoweights as well as for the max-fractional weight. The enumeration of codes and parity-check matrices can be described by the following algorithm.

Input: Parameters n (code length), k (code dimension), ρ (number of rows of the output parity-check matrices), where $\rho \geq r \triangleq n - k$.

Output: For all codes of length n, dimension k, distance $d \geq 3$, and without zero coordinates, up to code equivalence: a list of all $\rho \times n$ parity-check matrices, up to parity-check matrix equivalence.

1) Collect the set X of all $r \times n$ matrices such that
   - they have different nonzero columns, ordered lexicographically,
   - there is no non-empty $\mathbb{F}_2$-sum of rows which has weight 0 or 1 *(this way, the matrices are of full rank and the minimum distance of the row space is at least 2)*.

2) Determine the orbits in X under the action of the group $\mathrm{GL}_r(2)$ of invertible $r \times r$ matrices over $\mathbb{F}_2$ *(this enumerates all codes with the required properties, up to equivalence; the codes are represented by parity-check matrices)*.

3) For each orbit $X_\mathcal{C}$, representing a code $\mathcal{C}$:
   a) Determine the suborbits in $X_\mathcal{C}$ under the action of the symmetric group S_r *(this enumerates all parity-check matrices without redundant rows, up to equivalence)*.
   b) For each representative $\boldsymbol{H}$ of the suborbits, collect all matrices enlarged by adding $\rho - r$ different redundant rows that are $\mathbb{F}_2$-sums of at least two rows of $\boldsymbol{H}$. Let $X_{\mathcal{C},\rho}$ be the union of all such $\rho \times n$ matrices.
   c) Determine the orbits in $X_{\mathcal{C},\rho}$ under the action of the symmetric group S_ρ, and output a representative for each orbit.

TABLE I

THE NUMBER OF BINARY $[n, k, d]$ CODES

WITH $d \geq 3$ AND WITHOUT ZERO COORDINATES

	$k = 1$	2	3	4	5
$n = 5$	1	1			
6	1	3	1		
7	1	4	4	1	
8	1	6	10	5	
9	1	8	23	23	5

This algorithm was implemented in the C programming language. The minimum pseudoweights for the various parity-check matrices were computed by using Maple 12 and the Convex package [8].

B. Results

We considered all binary linear codes up to length n with distance $d \geq 3$ and without zero coordinates, up to code equivalence. The number of those codes for given length n and dimension k is shown in Table I.

1) AWGNC pseudoweight: The following results were found to hold for all codes of length $n \leq 9$.

- There are only two codes $\mathcal{C}$ with $\rho_{\text{AWGNC}}(\mathcal{C}) > r$, i.e. in class 0 or 1 for the AWGNC.
  - The $[8, 4, 4]$ extended Hamming code is the shortest code $\mathcal{C}$ in class 1. We have $\rho_{\text{AWGNC}}(\mathcal{C}) = 5 > 4 = r$ and out of 12 possible parity-check matrices (up to equivalence) with one redundant row there is exactly one matrix $\boldsymbol{H}$ with $\mathsf{w}^{\min}_{\text{AWGNC}}(\boldsymbol{H}) = 4$, namely

$$\boldsymbol{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} .$$

  There is exactly one matrix $\boldsymbol{H}$ with $\mathsf{w}^{\min}_{\text{AWGNC}}(\boldsymbol{H}) = 25/7$, and for the remaining matrices $\boldsymbol{H}$ we have $\mathsf{w}^{\min}_{\text{AWGNC}}(\boldsymbol{H}) = 3$.
  - Out of the four $[9, 4, 4]$ codes there is one code $\mathcal{C}$ in class 1. We have $\rho_{\text{AWGNC}}(\mathcal{C}) = 6 > 5 = r$ and out of 2526 possible parity-check matrices (up to equivalence) with one redundant row there are 13 matrices $\boldsymbol{H}$ with $\mathsf{w}^{\min}_{\text{AWGNC}}(\boldsymbol{H}) = 4$.

- For all codes $\mathcal{C}$ of minimum distance $d \geq 3$ and for all parity-check matrices $\boldsymbol{H}$ of $\mathcal{C}$ we have $\mathsf{w}^{\min}_{\text{AWGNC}}(\boldsymbol{H}) \geq 3$; in particular, if $d = 3$, then $\mathcal{C}$ is in class 3 for the AWGNC.

- For the $[7, 3, 4]$ simplex code there is (up to equivalence) only one parity-check matrix $\boldsymbol{H}$ without redundant rows such that $\mathsf{w}^{\min}_{\text{AWGNC}}(\boldsymbol{H}) = 4$, namely

$$\boldsymbol{H} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} .$$

It is the only parity-check matrix with constant row weight 3.

2) BSC pseudoweight: We computed the pseudocodeword redundancy for the BSC for all codes of length $n \leq 8$.

- The shortest codes with $\rho_{\text{BSC}}(\mathcal{C}) > r$, i.e. in class 0 or 1 for the BSC, are the $[7, 4, 3]$ Hamming code $\mathcal{C}$ and its dual code $\mathcal{C}^{\perp}$, the $[7, 3, 4]$ simplex code. We have $\rho_{\text{BSC}}(\mathcal{C}) = 4 > 3$ and $\rho_{\text{BSC}}(\mathcal{C}^{\perp}) = 5 > 4$.

- There are two codes of length 8 with $\rho_{\text{BSC}}(\mathcal{C}) > r$. These are the $[8, 4, 4]$ extended Hamming code, for which $\rho_{\text{BSC}}(\mathcal{C}) = 6 > 4$ holds, and one of the three $[8, 3, 4]$ codes, which satisfies $\rho_{\text{BSC}}(\mathcal{C}) = 6 > 5$.

3) Max-fractional weight: We computed the pseudocodeword redundancy with respect to the max-fractional weight for all codes of length $n \leq 8$.

- The shortest code with $\rho_{\text{max-frac}}(\mathcal{C}) > r$ is the unique $[6, 3, 3]$ code $\mathcal{C}$. We have $\rho_{\text{max-frac}}(\mathcal{C}) = 4 > 3$.

- There are two codes of length 7 with $\rho_{\text{max-frac}}(\mathcal{C}) > r$. These are the $[7, 4, 3]$ Hamming code and the $[7, 3, 4]$ simplex code, which have both pseudocodeword redundancy 7. In both cases, there is, up to equivalence, a unique parity-check matrix $\boldsymbol{H}$ with seven rows that satisfies $d(\mathcal{C}) = w^{\min}_{\text{max-frac}}(\boldsymbol{H})$.
  (This demonstrates that Proposition 5.4 and 5.5 in [6] are sharp for the max-fractional weight, and that the parity-check matrices constructed in the proofs are unique in this case.)

- For the $[8, 4, 4]$ extended Hamming code $\mathcal{C}$ we have $\rho_{\text{max-frac}}(C) = \infty$, and thus the code is in class 0 for the max-fractional weight. It is the shortest code with infinite $\rho_{\text{max-frac}}(\mathcal{C})$.
  (It can be checked that $\boldsymbol{x} = [1, 1, 1, 1, 1, 1, 1, 3]$ is a pseudocodeword in $\mathcal{K}(\boldsymbol{H})$, where the rows of $\boldsymbol{H}$ consist of all dual codewords; since $\mathsf{w}_{\text{max-frac}}(\boldsymbol{x}) = \frac{10}{3} < 4$, we have $w^{\min}_{\text{max-frac}}(\boldsymbol{H}) < 4$.)

- There are two other codes of length 8 with $\rho_{\text{max-frac}}(\mathcal{C}) > r$, namely two of the three $[8, 3, 4]$ codes, having pseudocodeword redundancy 6 and 8, respectively.

4) Comparison: Comparing the results for the AWGNC and BSC pseudoweights, and the max-fractional weight, we can summarize the results as follows.

- For the $[7, 4, 3]$ Hamming code $\mathcal{C}$ we have $\rho_{\text{AWGNC}}(\mathcal{C}) = r = 3$, $\rho_{\text{BSC}}(\mathcal{C}) = 4$, and $\rho_{\text{max-frac}}(\mathcal{C}) = 7$.

- For the $[7, 3, 4]$ simplex code $\mathcal{C}$ we have $\rho_{\text{AWGNC}}(\mathcal{C}) = r = 4$, $\rho_{\text{BSC}}(\mathcal{C}) = 5$, and $\rho_{\text{max-frac}}(\mathcal{C}) = 7$.

- For the $[8, 4, 4]$ extended Hamming code $\mathcal{C}$ we have $\rho_{\text{AWGNC}}(\mathcal{C}) = 5$, $\rho_{\text{BSC}}(\mathcal{C}) = 6$, and $\rho_{\text{max-frac}}(\mathcal{C}) = \infty$. This code $\mathcal{C}$ is the shortest one such that $\rho_{\text{AWGNC}}(\mathcal{C}) > r$, and also the shortest one such that $\rho_{\text{max-frac}}(\mathcal{C}) = \infty$.

- If $d \geq 3$ then for *every* parity-check matrix $\boldsymbol{H}$ we have $\mathsf{w}^{\min}_{\text{AWGNC}}(\boldsymbol{H}) \geq 3$. This is not true for the BSC and the max-fractional weight.

These observations show that there is some significant difference between the various types of pseudocodeword redundancies.

VI. Cyclic Codes Meeting the Eigenvalue Bound

In this section we apply the following eigenvalue-based lower bound on the minimum AWGNC pseudoweight, proved in [9].

Proposition 6.1: The minimum AWGNC pseudoweight for a (w_c, w_r)-regular parity-check matrix $\boldsymbol{H}$ whose corresponding Tanner graph is connected is bounded below by

$$\mathsf{w}_{\text{AWGNC}}^{\min} \geq n \cdot \frac{2w_c - \mu_2}{\mu_1 - \mu_2} \;, \tag{6}$$

where μ_1 and μ_2 denote the largest and second largest eigenvalue (respectively) of the matrix $\boldsymbol{L} \triangleq \boldsymbol{H}^T \boldsymbol{H}$, considered as a matrix over the real numbers.

We consider now binary cyclic codes with full circulant parity-check matrices, defined as follows: Let $\mathcal{C}$ be a binary cyclic code of length n with check polynomial $h(x) = \sum_{i \in \mathcal{I}} h_i x^i$ (cf. [10], p. 194). Then the *full circulant parity-check matrix* for $\mathcal{C}$ is the $n \times n$ matrix $\boldsymbol{H} = (H_{j,i})_{i,j \in \mathcal{I}}$ with entries $H_{j,i} = h_{j-i}$. Here, all the indices are modulo n, so that $\mathcal{I} = \{0, 1, \ldots, n-1\}$.

Since such a matrix is w-regular, where $w = \sum_{i \in \mathcal{I}} h_i$, we may use the eigenvalue-based lower bound of Proposition 6.1 to examine the AWGNC pseudocodeword redundancy: If the right hand side equals the minimum distance d of the code $\mathcal{C}$, then $\rho_{\text{AWGNC}}(\mathcal{C}) \leq n$.

Note that the largest eigenvalue of the matrix $\boldsymbol{L} = \boldsymbol{H}^T \boldsymbol{H}$ is $\mu_1 = w^2$, since every row weight of $\boldsymbol{L}$ equals $\sum_{i,j \in \mathcal{I}} h_i h_j = w^2$. Consequently, the eigenvalue bound is

$$\mathsf{w}_{\text{AWGNC}}^{\min} \geq n \cdot \frac{2w - \mu_2}{w^2 - \mu_2} \;,$$

where μ_2 is the second largest eigenvalue of $\boldsymbol{L}$. We remark further that $\boldsymbol{L} = (L_{j,i})_{i,j \in \mathcal{I}}$ is a symmetric circulant matrix, with $L_{j,i} = \ell_{j-i}$ and $\ell_i = \sum_{k \in \mathcal{I}} h_k h_{k+i}$. The eigenvalues of $\boldsymbol{L}$ are thus given by

$$\lambda_j = \sum_i \ell_i \zeta_n^{ij} = \operatorname{Re} \sum_i \ell_i \zeta_n^{ij} = \sum_i \ell_i \cos(2\pi i j / n)$$

for $j \in \mathcal{I}$, where $\zeta_n = \exp(2\pi \boldsymbol{i}/n)$, $\boldsymbol{i}^2 = -1$, is the n-th root of unity (see e.g. [11], Theorem 3.2.2).

We also consider quasi-cyclic codes of the form given in the following remark.

Remark 6.2: Denote by $\boldsymbol{1}_m$ the $m \times m$ matrix with all entries equal to 1. If $\boldsymbol{H}$ is a w-regular circulant $n \times n$ matrix then the Kronecker product $\tilde{\boldsymbol{H}} \triangleq \boldsymbol{H} \otimes \boldsymbol{1}_m$ will be a w-regular circulant $mn \times mn$-matrix and defines a quasi-cyclic code. We have

$$\tilde{\boldsymbol{L}} = \tilde{\boldsymbol{H}}^T \tilde{\boldsymbol{H}} = \boldsymbol{H}^T \boldsymbol{H} \otimes \boldsymbol{1}_m^T \boldsymbol{1}_m = \boldsymbol{L} \otimes (m\boldsymbol{1}_m) \;,$$

and the eigenvalues of $m\boldsymbol{1}_m$ are m^2 and 0. Thus, the largest eigenvalues of $\tilde{\boldsymbol{L}}$ are $\tilde{\mu}_1 = m^2 \mu_1 = m^2 w^2$ and $\tilde{\mu}_2 = m^2 \mu_2$, and the eigenvalue bound of Proposition 6.1 becomes

$$\mathsf{w}_{\text{AWGNC}}^{\min} \geq mn \cdot \frac{2mw - m^2 \mu_2}{m^2 w^2 - m^2 \mu_2} = n \cdot \frac{2w - m\mu_2}{w^2 - \mu_2} \;.$$

We carried out an exhaustive search on all cyclic codes $\mathcal{C}$ up to length $n \leq 250$ and computed the eigenvalue bound in

TABLE II
BINARY CYCLIC CODES UP TO LENGTH 250 WITH $d = 2$
MEETING THE EIGENVALUE BOUND

parameters	w-regular	constituent code
$[2n, 2n-m, 2]$	2^m	Hamming c., $n = 2^m - 1$, $m = 2 \ldots 6$
$[2n, 2n-m-1, 2]$	$2^m - 2$	Hamming c. with overall p.-check
$[42, 32, 2]$	10	projective geometry code $PG(2,4)$
$[146, 118, 2]$	18	projective geometry code $PG(2,8)$
$[170, 153, 2]$	42	a certain $[85, 68, \geq 6]$ 21-regular code (the eigenvalue bound is 5.2)

TABLE III
BINARY CYCLIC CODES UP TO LENGTH 250 WITH $d \geq 3$
MEETING THE EIGENVALUE BOUND

parameters	w-regular	comments
$[n, 1, n]$	2	repetition code, $n = 3 \ldots 250$
$[n, n-m, 3]$	2^{m-1}	Hamming c., $n = 2^m - 1$, $m = 3 \ldots 7$
$[7, 3, 4]$	3	dual of the $[7, 4, 3]$ Hamming code
$[15, 7, 5]$	4	Euclidean geometry code EG(2,4)
$[21, 11, 6]$	5	projective geometry code PG(2,4)
$[63, 37, 9]$	8	Euclidean geometry code EG(2,8)
$[73, 45, 10]$	9	projective geometry code PG(2,8)

all cases where the Tanner graph of the full circulant parity-check matrix is connected, by using the following algorithm:

Input: Parameter n (code length).
Output: For all divisors of $x^n - 1$, corresponding to cyclic codes $\mathcal{C}$ with full circulant parity-check matrix, such that the Tanner graph is connected: the value of the eigenvalue bound.

1) Factor $x^n - 1$ over $\mathbb{F}_2$ into irreducibles, using Cantor and Zassenhaus' algorithm (cf. [12], Section 14.3).
2) For each divisor $f(x)$ of $x^n - 1$:
   a) Let $f(x) = \sum_i h_i x^i$ and $\boldsymbol{H} = (h_{j-i})_{i,j \in \mathcal{I}}$.
   b) Check that the corresponding Tanner graph is connected (that the gcd of the indices i with $h_i = 1$ together with n is 1).
   c) Compute the eigenvalues of $\boldsymbol{L} = \boldsymbol{H}^T \boldsymbol{H}$: Let $\ell_i = \sum_{k \in \mathcal{I}} h_k h_{k+i}$ and for $j \in \mathcal{I}$ compute $\sum_i \ell_i \cos(2\pi i j / n)$.
   d) Determine the second largest eigenvalue μ_2 and output $n \cdot (2\ell_0 - \mu_2)/(\ell_0^2 - \mu_2)$.

This algorithm was implemented in the C programming language. Tables II and III give a complete list of all cases in which the eigenvalue bound equals the minimum Hamming distance d, for the cases $d = 2$ and $d \geq 3$ respectively. In particular, the AWGNC pseudoweight equals the minimum Hamming distance in these cases as well and thus we have for the pseudocodeword redundancy $\rho_{\text{AWGNC}}(\mathcal{C}) \leq n$. All examples of distance 2 are actually quasi-cyclic codes as in Remark 6.2 with parity-check matrix $\tilde{\boldsymbol{H}} = \boldsymbol{H} \otimes \boldsymbol{1}_2$. We list here the constituent code given by the parity-check matrix $\boldsymbol{H}$.

We conclude this section by proving a result which was observed by the experiments.

Lemma 6.3: Let $m \geq 3$ and let $\mathcal{C}$ be the intersection of a Hamming code of length $n = 2^m - 1$ with a simple parity-check code of length n, which is a cyclic $[n, n - m - 1, 4]$ code. Consider its full circulant parity-check matrix $\boldsymbol{H}$. Then

$$\mathsf{w}_{\text{AWGNC}}^{\min}(\boldsymbol{H}) \geq 3 + \frac{1}{2^{m-2} - 1} > 3 .$$

In particular, if $m = 3$ then $\mathcal{C}$ is the $[7, 3, 4]$ code and the result implies $\mathsf{w}_{\text{AWGNC}}^{\min}(\boldsymbol{H}) = 4$ and $\rho_{\text{AWGNC}}(\mathcal{C}) \leq n$.

Proof: Let $\boldsymbol{H}$ be the w-regular full circulant parity-check matrix for $\mathcal{C}$. We claim that $w = 2^{m-1} - 1$. Indeed, each row $\boldsymbol{h}$ of $\boldsymbol{H}$ is a codeword of the dual code $\mathcal{C}^{\perp}$, and since $\mathcal{C}^{\perp}$ consists of the codewords of the simplex code and their complements, the weight of $\boldsymbol{h}$ and thus w must be $2^{m-1} - 1$, 2^{m-1}, or $2^m - 1$. But w cannot be even, for otherwise all codewords of $\mathcal{C}^{\perp}$ would be of even weight. As $w = 2^m - 1$ is clearly impossible, it must hold $w = 2^{m-1} - 1$.

Next, we show that the second largest eigenvalue of $\boldsymbol{L} = \boldsymbol{H}^T \boldsymbol{H} = (L_{j,i})_{i,j \in \mathcal{I}}$ equals $\mu_2 = 2^{m-2}$. Indeed, let $\boldsymbol{h}_1$ and $\boldsymbol{h}_2$ be different rows of $\boldsymbol{H}$, representing codewords of $\mathcal{C}^{\perp}$. As their weight is equal, their Hamming distance is even, and thus it must be 2^{m-1}. Hence, the size of the intersection of the supports of $\boldsymbol{h}_1$ and $\boldsymbol{h}_2$ is $2^{m-2} - 1$. This implies that $L_{i,i} = w$ and $L_{j,i} = 2^{m-2} - 1$, for $i \neq j$. Consequently, $\boldsymbol{L}$ has an eigenvalue of multiplicity $n - 1$, namely $w - (2^{m-2} - 1) = 2^{m-2}$, and thus μ_2 must be 2^{m-2}.

Finally, we apply Proposition 6.1 to get

$$\mathsf{w}_{\text{AWGNC}}^{\min} \geq (2^m - 1) \frac{2\left(2^{m-1} - 1\right) - 2^{m-2}}{(2^{m-1} - 1)^2 - 2^{m-2}} = 3 + \frac{1}{2^{m-2} - 1} .$$

∎

REFERENCES

[1] R. Koetter, W.-C. W. Li, P. O. Vontobel, and J. L. Walker, "Characterizations of pseudo-codewords of (low-density) parity-check codes," *Advances in Mathematics*, vol. 213, pp. 205–229, Aug. 2007.

[2] P. O. Vontobel and R. Koetter, "Graph-cover Decoding and Finite-Length Analysis of Message-Passing Iterative Decoding of LDPC Codes," accepted for *IEEE Trans. Inform. Theory*. Also available as ArXiv report at `arXiv:cs.IT/0512078`.

[3] G. D. Forney, R. Koetter, F. R. Kschischang, and A. Reznik, "On the Effective Weights of Pseudocodewords for Codes Defined on Graphs with Cycles," in *Codes, Systems, and Graphical Models*, IMA workshop, Minneapolis, USA, Aug. 1999. New York, USA: Springer, 2001, pp. 101–112.

[4] M. Schwartz and A. Vardy, "On the Stopping Distance and the Stopping Redundancy of Codes," *IEEE Trans. Inform. Theory*, vol. 52, no. 3, 2006, pp. 922–932.

[5] C. Kelley and D. Sridhara, "On the pseudocodeword weight and parity-check matrix redundancy of linear codes", in *Proc. IEEE Information Theory Workshop (ITW)*, Lake Tahoe, USA, Sep. 2007.

[6] J. Zumbrägel, M. F. Flanagan, and V. Skachek, "On the Pseudocodeword Redundancy", to appear in *Proc. IEEE International Symposium on Information Theory (ISIT)*, Austin, USA, June 2010. Also available as ArXiv report at `http://arxiv.org/abs/1001.1705`.

[7] J. Feldman, M. J. Mainwright, and D. R. Karger, "Using linear programming to decode binary linear codes," *IEEE Trans. Inform. Theory*, vol. 51, no. 3, 2005, pp. 954–972.

[8] M. Franz, "Convex - a Maple package for convex geometry," Version 1.1 (2009). Available at `http://www-fourier.ujf-grenoble.fr/~franz/convex`.

[9] P. O. Vontobel and R. Koetter, "Lower Bounds on the Minimum Pseudo-Weight of Linear Codes," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, Chicago, USA, June/July 2004, p. 67.

[10] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam, The Netherlands: North-Holland, 1978.

[11] P. J. Davis, *Circulant Matrices*, New York, USA: John Wiley & Sons, 1979.

[12] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra* (2nd ed.), Cambridge, United Kingdom: Cambridge University Press, 2003.