ISIT 2009, Seoul, Korea, June 28 - July 3, 2009

Absdet-Pseudo-Codewords and Perm-Pseudo-Codewords: Definitions and Properties

Roxana Smarandache*
Department of Mathematics and Statistics
San Diego State University
San Diego, CA 92182, USA
Email: rsmarand@sciences.sdsu.edu

Pascal O. Vontobel
Hewlett–Packard Laboratories
1501 Page Mill Road
Palo Alto, CA 94304, USA
Email: pascal.vontobel@ieee.org

***Abstract*—The linear-programming decoding performance of a binary linear code crucially depends on the structure of the fundamental cone of the parity-check matrix that describes the code. Towards a better understanding of fundamental cones and the vectors therein, we introduce the notion of absdet-pseudo-codewords and perm-pseudo-codewords: we give the definitions, we discuss some simple examples, and we list some of their properties.**

***Index Terms*—Absdet-pseudo-codeword, fundamental cone, low-density parity-check code, message-passing iterative decoding, perm-pseudo-codeword, pseudo-codeword, Tanner graph.**

I. Introduction

In [1], MacKay and Davey discussed a simple technique for upper bounding the minimum Hamming distance of a binary linear code that is described by a parity-check matrix. Their technique was based on explicitly constructing codewords and on using the fact that the Hamming weight of a non-zero codeword is an upper bound on the minimum Hamming distance of the code. This approach was subsequently extended and refined in the papers [2] and [3]. (Note that [1]–[3] focused mostly on quasi-cyclic binary linear codes, however, the technique is more generally applicable since any binary linear code of length n can trivially be considered to be a quasi-cyclic code with period n.)

In the technique by MacKay and Davey, the constructed codewords are binary vectors whose entries stem from certain determinants that are computed over the binary field. One wonders what happens if these determinants are not computed over the binary field but over the ring of integers. Do the resulting integer vectors still say something useful about the code under investigation? In this paper we answer this question affirmatively by showing that the resulting vectors (after replacing the components by their absolute value) are pseudo-codewords, i.e., vectors that lie in the fundamental cone of the parity-check matrix of the code. These pseudo-codewords, in the following called absdet-pseudo-codewords, are therefore important in the characterization of the performance of linear programming decoding [4], [5] and message-passing iterative decoding [6], [7].

The remainder of the paper is structured as follows. In Section II we list basic notations and definitions. Then, in Section III we formally define the class of absdet-pseudo-codewords and a closely related class of pseudo-codewords, so-called perm-pseudo-codewords. In order to get some initial understanding of these pseudo-codewords, in Section IV we construct them for some small codes. Afterwards, in Section V we discuss properties of these pseudo-codewords. We conclude the paper in Section VI.

* Supported by NSF Grants DMS-0708033 and TF-0830608.

II. Basic Notations and Definitions

Let $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{F}_2$ be the ring of integers, the field of real numbers, and the finite field of size 2, respectively. If $\mathbf{a}$ is some vector with integer entries, then $\mathbf{a} \pmod 2$ will denote an equally long vector whose entries are reduced modulo 2. Rows and columns of matrices and entries of vectors will be indexed starting at 0. If $\mathbf{M}$ is some matrix and if $\mathcal{R}$ and $\mathcal{S}$ are subsets of the row and column index sets, respectively, then $\mathbf{M}_{\mathcal{R},\mathcal{S}}$ is the sub-matrix of $\mathbf{M}$ that contains only the rows of $\mathbf{M}$ whose index appears in the set $\mathcal{R}$ and only the columns of $\mathbf{M}$ whose index appears in the set $\mathcal{S}$. If $\mathcal{R}$ equals the set of all row indices of $\mathbf{M}$, we will simply write $\mathbf{M}_{\mathcal{S}}$ instead of $\mathbf{M}_{\mathcal{R},\mathcal{S}}$. Moreover, we will use the short-hand $\mathcal{S} \setminus i$ for $\mathcal{S} \setminus \{i\}$.

Definition 1 *Let $\mathbf{M} = (m_{j,i})_{j,i}$ be an $n \times n$-matrix over some ring. Its determinant is defined to be*

$$\det(\mathbf{M}) = \sum_{\sigma} \operatorname{sgn}(\sigma) \prod_{j=0}^{n-1} m_{j,\sigma(j)} ,$$

where the summation is over all $n!$ permutations of the set $\{0, 1, \ldots, n-1\}$, and where $\operatorname{sgn}(\sigma)$ equals $+1$ if σ is an even permutation and equals -1 if σ is an odd permutation. Similarly, the permanent of $\mathbf{M}$ is defined to be

$$\operatorname{perm}(\mathbf{M}) = \sum_{\sigma} \prod_{j=0}^{n-1} m_{j,\sigma(j)} .$$

Clearly, for any matrix $\mathbf{M}$ with elements from a ring or field of characteristic 2 it holds that $\det(\mathbf{M}) = \operatorname{perm}(\mathbf{M})$.

When we want to emphasize that the matrix $\mathbf{M}$, of which we are computing the determinant or the permanent, is to be considered to be a matrix over the ring of integers, then we will write $\det_{\mathbb{Z}}(\mathbf{M})$ and $\operatorname{perm}_{\mathbb{Z}}(\mathbf{M})$, respectively. Note that $\det_{\mathbb{Z}}(\mathbf{M}) \pmod 2 = \operatorname{perm}_{\mathbb{Z}}(\mathbf{M}) \pmod 2$. □

Let $\mathbf{H} = (h_{j,i})_{j,i}$ be a parity-check matrix of some binary linear code. We define the sets $\mathcal{J}(\mathbf{H})$ and $\mathcal{I}(\mathbf{H})$ to be the set of row and column indices of $\mathbf{H}$. Moreover, we will use the sets $\mathcal{J}_i(\mathbf{H}) \triangleq \{j \in \mathcal{J} \mid h_{j,i} = 1\}$ and $\mathcal{I}_j(\mathbf{H}) \triangleq \{i \in \mathcal{I} \mid h_{j,i} = 1\}$. The Tanner graph that is associated to $\mathbf{H}$ will be denoted by $\mathsf{T}(\mathbf{H})$; the graph distance of bit nodes X_i and bit nodes $X_{i'}$ in $\mathsf{T}(\mathbf{H})$ will then be denoted by $d_{\mathsf{T}(\mathbf{H})}(X_i, X_{i'})$. (Note that this latter quantity is always a non-negative even integer.) In the following, when no confusion can arise, we will sometimes omit the argument $\mathbf{H}$ in the preceding expressions.

Definition 2 *The fundamental cone $\mathcal{K}(\mathbf{H})$ of $\mathbf{H}$ is the set of all vectors $\boldsymbol{\omega} \in \mathbb{R}^n$ that satisfy*

$$\omega_i \geqslant 0 \qquad \text{(for all } i \in \mathcal{I}(\mathbf{H})\text{)}\,, \tag{1}$$

$$\omega_i \leqslant \sum_{i' \in \mathcal{I}_j \setminus i} \omega_{i'} \quad \text{(for all } j \in \mathcal{J}(\mathbf{H}),\ \text{for all } i \in \mathcal{I}_j(\mathbf{H})\text{)}\,. \tag{2}$$

A vector $\boldsymbol{\omega} \in \mathcal{K}(\mathbf{H})$ is called a pseudo-codeword. If such a vector lies on an edge of $\mathcal{K}(\mathbf{H})$, it is called a minimal pseudo-codeword. Moreover, if $\boldsymbol{\omega} \in \mathcal{K}(\mathbf{H}) \cap \mathbb{Z}^n$ and $\boldsymbol{\omega} \pmod 2 \in \mathcal{C}$, then $\boldsymbol{\omega}$ is called an unscaled pseudo-codeword. (For a motivation of these definitions, see [7], [8]). □

Although the region in the log-likelihood ratio vector space where linear-programming decoding decides for the all-zero codeword is completely characterized by the minimal pseudo-codewords of $\mathcal{K}(\mathbf{H})$, the knowledge of non-minimal pseudo-codewords is also valuable since such pseudo-codewords can be used to bound this decision region.

III. Definition of Absdet-Pseudo-Codewords and Perm-Pseudo-Codewords

We start with the definition of det-vectors, absdet-vectors, and perm-vectors. As we will see, the properties of these vectors will then allow us to rename absdet-vectors and perm-vectors into absdet-pseudo-codewords and perm-pseudo-codewords, respectively.

Definition 3 *Let $\mathcal{C}$ be a binary linear code described by a parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{m \times n}$, $m < n$. For a size-$(m+1)$ subset $\mathcal{S}$ of $\mathcal{I}(\mathbf{H})$ we define the det-vector based on $\mathcal{S}$ to be the vector $\boldsymbol{\nu} \in \mathbb{Z}^n$ with components*

$$\nu_i \triangleq \begin{cases} (-1)^{\eta_{\mathcal{S}}(i)} \mathrm{det}_{\mathbb{Z}}(\mathbf{H}_{\mathcal{S}\setminus i}) & \text{if } i \in \mathcal{S} \\ 0 & \text{otherwise} \end{cases},$$

where $\eta_{\mathcal{S}}(i) \in \{0, 1, \ldots, |\mathcal{S}|-1\}$ is the index of i within the set $\mathcal{S}$. □

Definition 4 *Let $\mathcal{C}$ be a binary linear code described by a parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{m \times n}$, $m < n$. For a size-$(m+1)$ subset $\mathcal{S}$ of $\mathcal{I}(\mathbf{H})$ we define the absdet-vector based on $\mathcal{S}$ to be the vector $\boldsymbol{\omega} \in \mathbb{Z}^n$ with components*

$$\omega_i \triangleq \begin{cases} \left|\mathrm{det}_{\mathbb{Z}}(\mathbf{H}_{\mathcal{S}\setminus i})\right| & \text{if } i \in \mathcal{S} \\ 0 & \text{otherwise} \end{cases}.$$

□

Definition 5 *Let $\mathcal{C}$ be a binary linear code described by a parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{m \times n}$, $m < n$. For a size-$(m+1)$ subset $\mathcal{S}$ of $\mathcal{I}(\mathbf{H})$ we define the perm-vector based on $\mathcal{S}$ to be the vector $\boldsymbol{\omega} \in \mathbb{Z}^n$ with components*

$$\omega_i \triangleq \begin{cases} \mathrm{perm}_{\mathbb{Z}}(\mathbf{H}_{\mathcal{S}\setminus i}) & \text{if } i \in \mathcal{S} \\ 0 & \text{otherwise} \end{cases}.$$

□

Note that whereas det-vectors depend on the row ordering of a parity-check matrix, absdet-vectors and perm-vectors do not.

Before proving some lemmas and theorems about these vectors, let us state and prove an auxiliary result.

Lemma 6 *Let $\mathcal{C}$ be a binary linear code described by the parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{m \times n}$, and let $\boldsymbol{\nu} \in \mathbb{R}^n$ be a vector that satisfies*

$$\mathbf{H} \cdot \boldsymbol{\nu}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}} \quad \text{(in } \mathbb{R}\text{)}\,. \tag{3}$$

Then the vector $\boldsymbol{\omega} \in \mathbb{R}^n$ with components $\omega_i \triangleq |\nu_i|$, $i \in \mathcal{I}$, satisfies $\boldsymbol{\omega} \in \mathcal{K}(\mathbf{H})$.

Proof: In order to show that such a vector $\boldsymbol{\omega}$ is indeed in the fundamental cone of $\mathbf{H}$, we need to verify (1) and (2). The way $\boldsymbol{\omega}$ is defined, it is clear that it satisfies (1). Therefore, let us focus on the proof that $\boldsymbol{\omega}$ satisfies (2). Namely, from (3) it follows that for all $j \in \mathcal{J}$, $\sum_{i \in \mathcal{I}} h_{j,i} \nu_i = 0$, i.e., for all $j \in \mathcal{J}$, $\sum_{i \in \mathcal{I}_j} \nu_i = 0$. This implies

$$\omega_i = |\nu_i| = \left| - \sum_{i' \in \mathcal{I}_j \setminus i} \nu_{i'} \right| \leqslant \sum_{i' \in \mathcal{I}_j \setminus i} |\nu_{i'}| = \sum_{i' \in \mathcal{I}_j \setminus i} \omega_{i'}$$

for all $j \in \mathcal{J}$ and all $i \in \mathcal{I}_j$, showing that $\boldsymbol{\omega}$ indeed satisfies (2). ■

Lemma 7 *Let $\mathcal{C}$ be a binary linear code described by the parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{m \times n}$, $m < n$, and let $\mathcal{S}$ be a size-$(m+1)$ subset of $\mathcal{I}(\mathbf{H})$. The det-vector $\boldsymbol{\nu}$ based on $\mathcal{S}$ satisfies*

$$\mathbf{H} \cdot \boldsymbol{\nu}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}} \quad \text{(in } \mathbb{Z}\text{)}\,, \tag{4}$$

$$\boldsymbol{\nu} \pmod 2 \in \mathcal{C}\,. \tag{5}$$

Proof: Let $\mathbf{s}^{\mathsf{T}} \triangleq \mathbf{H} \cdot \boldsymbol{\nu}^{\mathsf{T}}$ (in $\mathbb{Z}$) be the $\mathbb{Z}$-syndrome. Then, by the definition of the det-vector in Definition 3

$$s_j = \sum_{i \in \mathcal{I}} h_{j,i} \nu_i = \sum_{i \in \mathcal{S}} (-1)^{\eta_{\mathcal{S}}(i)} h_{j,i} \mathrm{det}_{\mathbb{Z}}(\mathbf{H}_{\mathcal{S}\setminus i})\,,$$

for any $j \in \mathcal{J}(\mathbf{H})$. Let $\mathcal{S} = \{i_0, i_1, \ldots, i_m\} \subseteq \mathcal{I}(\mathbf{H})$. Observing that s_j is the the co-factor expansion of the $\mathbb{Z}$-determinant of the $(m+1) \times (m+1)$-matrix

$$\begin{bmatrix} h_{j,i_0} & h_{j,i_1} & \cdots & h_{j,i_m} \\ \hline h_{0,i_0} & h_{0,i_1} & \cdots & h_{0,i_m} \\ h_{1,i_0} & h_{1,i_1} & \cdots & h_{1,i_m} \\ \vdots & \vdots & \cdots & \vdots \\ h_{m-1,i_0} & h_{m-1,i_1} & \cdots & h_{m-1,i_m} \end{bmatrix}, \tag{6}$$

and noting that this latter matrix is singular (because at least two rows are equal), we obtain the result that $\mathbf{s} = \mathbf{0}$, as promised.

The proof of (5) follows by noticing that $\mathbf{H}\cdot\boldsymbol{\nu}^\mathsf{T} = \mathbf{0}^\mathsf{T}$ (in $\mathbb{Z}$) implies that $\mathbf{H}\cdot\big(\boldsymbol{\nu} \pmod 2\big)^\mathsf{T} \pmod 2 = \mathbf{0}^\mathsf{T}$. ■

Theorem 8 *Let $\mathcal{C}$ be a binary linear code described by the parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{m\times n}$, $m < n$, and let $\mathcal{S}$ be a size-$(m{+}1)$ subset of $\mathcal{I}(\mathbf{H})$. The absdet-vector $\boldsymbol{\omega}$ based on $\mathcal{S}$ is an unscaled pseudo-codeword of $\mathbf{H}$, i.e.,*

$$\boldsymbol{\omega} \in \mathcal{K}(\mathbf{H})\,, \tag{7}$$

$$\boldsymbol{\omega} \pmod 2 \in \mathcal{C}\,. \tag{8}$$

Proof: Let $\boldsymbol{\nu}$ be the det-vector based on $\mathcal{S}$. From Lemma 7 we know that $\boldsymbol{\nu}$ satisfies $\mathbf{H}\cdot\boldsymbol{\nu}^\mathsf{T} = \mathbf{0}^\mathsf{T}$ (in $\mathbb{Z}$). Because of this, and because $\omega_i = |\nu_i|$ for $i \in \mathcal{I}$, we can use Lemma 6 to conclude that indeed $\boldsymbol{\omega} \in \mathcal{K}(\mathbf{H})$.

Finally, (8) is verified as follows. Lemma 7 shows that $\boldsymbol{\nu} \pmod 2 \in \mathcal{C}$, which, upon noticing that $\boldsymbol{\nu} \pmod 2 = \boldsymbol{\omega} \pmod 2$, implies that $\boldsymbol{\omega} \pmod 2 \in \mathcal{C}$. ■

Theorem 9 *Let $\mathcal{C}$ be a binary linear code described by the parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{m\times n}$, $m < n$, and let $\mathcal{S}$ be a size-$(m{+}1)$ subset of $\mathcal{I}(\mathbf{H})$. The perm-vector $\boldsymbol{\omega}$ based on $\mathcal{S}$ is an unscaled pseudo-codeword of $\mathbf{H}$, i.e.,*

$$\boldsymbol{\omega} \in \mathcal{K}(\mathbf{H})\,, \tag{9}$$

$$\boldsymbol{\omega} \pmod 2 \in \mathcal{C}\,. \tag{10}$$

Proof: In order to show (9), we need to verify (1) and (2). From Definition 5 it is clear that $\boldsymbol{\omega}$ satisfies (1). Therefore, let us focus on the proof that $\boldsymbol{\omega}$ satisfies (2). Fix some $j \in \mathcal{J}(\mathbf{H})$ and some $i \in \mathcal{I}_j(\mathbf{H})$. If $i \notin \mathcal{S}$ then $\omega_i = 0$ and (2) is clearly satisfied. Therefore, assume that $i \in \mathcal{S}$. Then

$$\begin{aligned}
\sum_{i' \in \mathcal{I}_j \setminus i} \omega_{i'} &= \sum_{i' \in \mathcal{I} \setminus i} h_{j,i'} \omega_{i'} \\
&= \sum_{i' \in \mathcal{S} \setminus i} h_{j,i'} \cdot \mathrm{perm}_{\mathbb{Z}}\big(\mathbf{H}_{\mathcal{S}\setminus i'}\big) + \sum_{i' \in (\mathcal{I}\setminus\mathcal{S})\setminus i} h_{j,i'} \cdot 0 \\
&= \sum_{i' \in \mathcal{S} \setminus i} h_{j,i'} \sum_{i'' \in \mathcal{S} \setminus i'} h_{j,i''} \mathrm{perm}_{\mathbb{Z}}\big(\mathbf{H}_{\mathcal{J}\setminus j, \mathcal{S}\setminus\{i',i''\}}\big) \\
&\overset{(*)}{\geqslant} \sum_{i' \in \mathcal{S} \setminus i} h_{j,i'} h_{j,i} \mathrm{perm}_{\mathbb{Z}}\big(\mathbf{H}_{\mathcal{J}\setminus j, \mathcal{S}\setminus\{i',i\}}\big) \\
&= h_{j,i} \sum_{i' \in \mathcal{S} \setminus i} h_{j,i'} \mathrm{perm}_{\mathbb{Z}}\big(\mathbf{H}_{\mathcal{J}\setminus j, \mathcal{S}\setminus\{i',i\}}\big) \\
&= h_{j,i} \mathrm{perm}_{\mathbb{Z}}\big(\mathbf{H}_{\mathcal{S}\setminus i}\big) = h_{j,i}\omega_i \overset{(**)}{=} \omega_i\,,
\end{aligned}$$

where at step $(*)$ we kept only the terms for which $i'' = i$, and where step $(**)$ follows from $i \in \mathcal{I}_j(\mathbf{H})$. Because $j \in \mathcal{J}(\mathbf{H})$ and $i \in \mathcal{I}_j(\mathbf{H})$ were arbitrary, $\boldsymbol{\omega}$ indeed satisfies (2).

Finally, (10) is verified as follows. Let $\boldsymbol{\nu}$ be the det-vector based on $\mathcal{S}$. Lemma 7 shows that $\boldsymbol{\nu} \pmod 2 \in \mathcal{C}$, which, upon noticing that $\boldsymbol{\nu} \pmod 2 = \boldsymbol{\omega} \pmod 2$, implies that $\boldsymbol{\omega} \pmod 2 \in \mathcal{C}$. ■

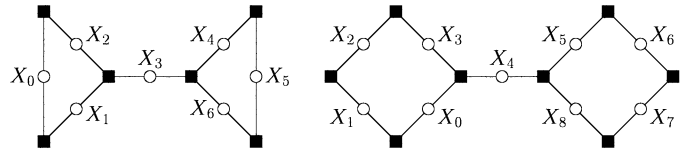

Figure 1. Tanner graphs of dumbbell-graph-based codes. Left: $[7, 2, 3]$ binary linear code. Right: $[9, 2, 4]$ binary linear code.

Definition 10 *Because of Theorems 8 and 9, absdet-vectors and perm-vectors will henceforth be called absdet-pseudo-codewords and perm-pseudo-codewords, respectively.* □

IV. Examples

In order to get a better feeling of what absdet-pseudo-codewords and perm-pseudo-codewords look like, let us discuss some examples.

Example 11 Consider the $[4, 2, 2]$ binary linear code $\mathcal{C}$ based on the parity-check matrix $\mathbf{H} \triangleq \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$, where $n = 4$ and $m = 2$. Let us compute the absdet-pseudo-codewords and perm-pseudo-codewords for all possible subsets $\mathcal{S}$ of $\mathcal{I}(\mathbf{H})$ of size $m{+}1 = 3$. We obtain the following list of absdet-pseudo-codewords: $(0, 1, 1, 0)$ (twice), $(1, 1, 0, 1)$, $(1, 0, 1, 1)$. These happen to be all the non-zero codewords of $\mathcal{C}$. Moreover, this parity-check matrix yields the following list of perm-pseudo-codewords: $(2, 1, 1, 0)$, $(1, 1, 0, 1)$, $(1, 0, 1, 1)$, $(0, 1, 1, 2)$. Note that, up to scaling, $(2, 1, 1, 0)$ and $(0, 1, 1, 2)$ are the only non-codeword minimal pseudo-codewords of $\mathcal{K}(\mathbf{H})$. □

Example 12 Consider the dumbbell-graph-based $[7, 2, 3]$ binary linear code described by the Tanner graph in Figure 1 (left) with $n = 7$ bit nodes and $m = 6$ check nodes. Obviously, there is only one subset $\mathcal{S}$ of $\mathcal{I}(\mathbf{H})$ of size $m{+}1 = 7 = n$, i.e. $\mathcal{S} = \mathcal{I}(\mathbf{H})$. This set $\mathcal{S}$ yields the absdet-pseudo-codeword $(2, 2, 2, 4, 2, 2, 2)$. Note that this is the only non-codeword minimal pseudo-codeword of $\mathcal{K}(\mathbf{H})$ (cf. [7], [8]). Moreover, for this example the perm-pseudo-codeword based on $\mathcal{S}$ happens to be also $(2, 2, 2, 4, 2, 2, 2)$. □

Example 13 Consider the dumbbell-graph-based $[9, 2, 4]$ binary linear code described by the Tanner graph in Figure 1 (right) with $n = 9$ bit nodes and $m = 8$ check nodes. It yields the absdet-pseudo-codeword $(0, 0, 0, 0, 0, 0, 0, 0, 0)$ and the perm-pseudo-codewords $(2, 2, 2, 2, 4, 2, 2, 2, 2)$. Note that this latter vector is the only non-codeword minimal pseudo-codeword of $\mathcal{K}(\mathbf{H})$. □

Example 14 Consider a randomly generated $(3, 4)$-regular $[20, 5]$ LDPC code based on a 15×20 parity-check matrix $\mathbf{H}_1$ that potentially contains four-cycles. The blue curve (top curve) in Figure 2 shows the AWGNC pseudo-weight cumulative histogram of the absdet-pseudo-codewords of $\mathbf{H}_1$ based on all subsets $\mathcal{S}$ of $\mathcal{I}(\mathbf{H})$ of size $m{+}1 = 16$.

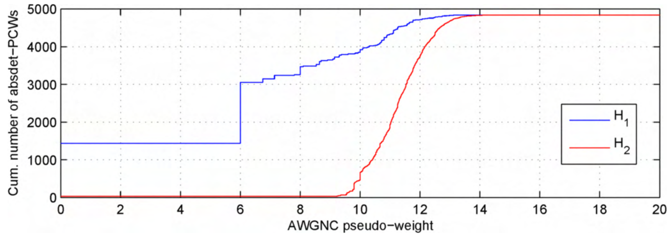

Figure 2. AWGNC pseudo-weight cumulative histograms of the absdet-PCWs (absdet-pseudo-codewords) of the parity-check matrices in Example 14. (The AWGNC pseudo-weight of a pseudo-codeword $\boldsymbol{\omega}$ is defined to be $w_{\mathrm{p}}^{\mathrm{AWGNC}}(\boldsymbol{\omega}) = \|\boldsymbol{\omega}\|_1^2/\|\boldsymbol{\omega}\|_2^2$ [6], [7].) Blue curve (top curve): $\mathbf{H}_1$. Red curve (bottom curve): $\mathbf{H}_2$.

Eliminating four-cycles in $\mathsf{T}(\mathbf{H}_1)$ by applying an edge-permutation procedure results in a Tanner graph $\mathsf{T}(\mathbf{H}_2)$ of a new code described by a parity-check matrix $\mathbf{H}_2$. The red curve (bottom curve) in Figure 2 shows the AWGNC pseudo-weight cumulative histogram of the absdet-pseudo-codewords of $\mathbf{H}_2$ based on all subsets $\mathcal{S}$ of $\mathcal{I}(\mathbf{H})$ of size $m+1 = 16$.

Comparing these two curves, we make the following observation: first, for $\mathbf{H}_1$ there are more absdet-pseudo-codewords than for $\mathbf{H}_2$ that equal the all-zero vector. As we will briefly discuss in the next section, this observation is related to the existence of four-cycles. Secondly, the curve related to $\mathbf{H}_1$ is to the left of the curve related to $\mathbf{H}_2$. This corroborates the common observation that codes based on Tanner graphs with four-cycles usually perform worse than codes based on Tanner graphs without four-cycles. $\square$

V. Properties of Absdet-Pseudo-Codewords and Perm-Pseudo-Codewords

In this section we discuss some properties of absdet-pseudo-codewords and of perm-pseudo-codewords. Some proofs are shortened or omitted due to space restrictions.

Remark 15 Using a well-known property of permanents of matrices with zeros and ones, it follows that the term $\mathrm{perm}_{\mathbb{Z}}(\mathbf{H}_{\mathcal{S}\setminus i})$, which appears in the definition of perm-vectors in Definition 5, equals the number of perfect matchings in the Tanner graph $\mathsf{T}(\mathbf{H}_{\mathcal{S}\setminus i})$. Moreover, because Theorem 9 showed that perm-vectors satisfy (2), we see that for every $j \in \mathcal{J}(\mathbf{H})$, Eq. (2) relates the set of perfect matchings in the Tanner graphs $\{\mathsf{T}(\mathbf{H}_{\mathcal{S}\setminus i})\}_{i\in\mathcal{I}_j(\mathbf{H})}$. $\square$

Theorem 16 *Let $\mathbf{H}$ be the parity-check matrix of a code whose associated Tanner graph is a tree, i.e., does not contain cycles. Then all entries of all absdet-pseudo-codewords and all entries of all perm-pseudo-codewords are either* 0 *or* 1.

Proof: (Sketch.) A necessary condition for the Tanner graph $\mathsf{T}(\mathbf{H}_{\mathcal{S}\setminus i})$ to have at least two perfect matchings is the existence of a cycle in the Tanner graph. However, if $\mathsf{T}(\mathbf{H})$ is cycle-free then also $\mathsf{T}(\mathbf{H}_{\mathcal{S}\setminus i})$ is cycle-free. For perm-pseudo-codewords the claim then follows from Remark 15.

Moreover, for any set $\mathcal{S}$, the entries of the absdet-pseudo-codeword are always upper bounded by the corresponding entries in the perm-pseudo-codeword, and so the claim also follows for absdet-pseudo-codewords. $\blacksquare$

Remark 17 For a parity-check matrix $\mathbf{H}$, the existence of short cycles in $\mathsf{T}(\mathbf{H})$ has an influence on the list of absdet-pseudo-codewords. In particular, without going into the details, four-cycles imply more absdet-pseudo-codewords that equal the all-zero codeword. Related statements can be made about six-cycles, eight-cycles, etc.. As part of future research, it will be interesting to formulate probabilistic statements that will help characterizing long codes where not all absdet-pseudo-codewords can be listed by brute-force techniques. $\square$

Remark 18 Note that the pseudo-codeword $(2, 2, 2, 4, 2, 2, 2)$ that was found in Example 12 can be seen as a canonical completion with root X_4 [6], [7]. (Strictly speaking, the canonical completion was only defined for check-degree regular codes, however, it is straightforward to suitably extend the canonical completion technique to Tanner graphs where the check nodes with the same graph distance to the root node have the same degree.)

More generally, one can establish the following connection between Lemma 6 and the canonical completion. Namely, let $\boldsymbol{\omega} \in \mathbb{R}^n$ be the canonical completion with root X_i for some $i \in \mathcal{I}(\mathbf{H})$ and define $\boldsymbol{\nu} \in \mathbb{R}^n$ such that

$$\nu_{i'} \triangleq \begin{cases} +\omega_{i'} & (\text{if } d_{\mathsf{T}(\mathbf{H})}(X_i, X_{i'}) \in 4\mathbb{Z}) \\ -\omega_{i'} & (\text{if } d_{\mathsf{T}(\mathbf{H})}(X_i, X_{i'}) \in 2\mathbb{Z} \setminus 4\mathbb{Z}) \end{cases}$$

for all $i' \in \mathcal{I}(\mathbf{H})$. (With this, $\boldsymbol{\omega}$ obviously satisfies $\omega_{i'} = |\nu_{i'}|$ for all $i' \in \mathcal{I}(\mathbf{H})$.) Let $\mathcal{J}'(\mathbf{H})$ be the subset of indices of check nodes that have only one neighboring bit node that is closer (in graph distance) to the root than they are to the root. It can then easily be verified that $\mathbf{H}_{\mathcal{J}',\mathcal{I}} \cdot \boldsymbol{\nu}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$, which, with the help of Lemma 6, implies that $\boldsymbol{\omega} \in \mathcal{K}(\mathbf{H}_{\mathcal{J}',\mathcal{I}})$. $\square$

The next theorem relates absdet-pseudo-codewords to quantities that appear naturally in a certain Gaussian graphical model associated to $\mathsf{T}(\mathbf{H})$. In order to motivate the Gaussian graphical model in that theorem, remember that a Tanner/factor graph of a code represents the indicator function $[\mathbf{x} \in \mathcal{C}] = \prod_{i\in\mathcal{I}} f'_i(x_i) \cdot \prod_{j\in\mathcal{J}} f''_j(\mathbf{x}_{\mathcal{I}_j})$ with $f'_i(x_i) \triangleq [x_i \in \{0,1\}]$ and $f''_j(\mathbf{x}_{\mathcal{I}_j}) \triangleq [\sum_{i\in\mathcal{I}_j} x_i \pmod 2 = 0]$, and that the indicator function of the fundamental cone can be written as $[\boldsymbol{\omega} \in \mathcal{K}(\mathbf{H})] = \prod_{i\in\mathcal{I}} k'_i(\omega_i) \cdot \prod_{j\in\mathcal{J}} k''_j(\boldsymbol{\omega}_{\mathcal{I}_j})$ with $k'_i(\omega_i) \triangleq [x_i \geqslant 0]$ and some suitably defined functions $k''_j(\mathbf{x}_{\mathcal{I}_j})$.

Theorem 19 *Let $\mathcal{C}$ be a binary linear code described by the parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{m\times n}$. For some arbitrary $\varepsilon > 0$, consider the Gaussian graphical model for the length-n vector $\mathbf{U}$ defined by $p_{\mathbf{U}}(\mathbf{u}) \propto \prod_{i\in\mathcal{I}} g'_i(u_i) \cdot \prod_{j\in\mathcal{J}} g''_j(\mathbf{u}_{\mathcal{I}_j})$ with*

$$g'_i(u_i) \triangleq \exp\left(-\frac{u_i^2}{2(1/\varepsilon)^2}\right),\ g''_j(\mathbf{u}_{\mathcal{I}_j}) \triangleq \exp\left(-\frac{1}{2}\sum_{(i,i')\in\mathcal{I}_j\times\mathcal{I}_j} u_i u_{i'}\right).$$

Let $\mathcal{S}$ be a size-$(m+1)$ subset of $\mathcal{I}(\mathbf{H})$ and let $\bar{\mathcal{S}} \triangleq \mathcal{I}(\mathbf{H}) \setminus \mathcal{S}$ be its complement. (We assume that $m < n$.) Let $\sigma_{i|\bar{\mathcal{S}}}(\varepsilon)$ be the square root of the minimum mean squared error when estimating U_i (with a linear or a non-linear estimator) based on the knowledge of $\mathbf{U}_{\bar{\mathcal{S}}} = \mathbf{u}_{\bar{\mathcal{S}}}$. Then the components of the absdet pseudo-codeword $\boldsymbol{\omega}$ based on $\mathcal{S}$ fulfill

$$\omega_i = \lim_{\varepsilon \to 0} \gamma_{\mathcal{S}|\bar{\mathcal{S}}}(\varepsilon) \cdot \sigma_{i|\bar{\mathcal{S}}}(\varepsilon) \tag{11}$$

for all $i \in \mathcal{I}(\mathbf{H})$, where $\gamma_{\mathcal{S},\bar{\mathcal{S}}}(\varepsilon)$ is a function of ε, but independent of $i \in \mathcal{I}(\mathbf{H})$.

Proof: First, we consider the case where $i \in \bar{\mathcal{S}}$. From Definition 4 we see that $\omega_i = 0$. On the other hand, U_i can perfectly be predicted based on the knowledge of of $\mathbf{U}_{\bar{\mathcal{S}}} = \mathbf{u}_{\bar{\mathcal{S}}}$, which implies $\sigma^2_{i|\bar{\mathcal{S}}}(\varepsilon) = 0$. Since $\gamma_{\mathcal{S},\bar{\mathcal{S}}}(\varepsilon)$ (defined below) is bounded for all suitably small $\varepsilon > 0$, we have proven (11) for $i \in \bar{\mathcal{S}}$.

Secondly, we consider the case where $i \in \mathcal{S}$. We start by noting that $p_{\mathbf{U}}(\mathbf{u})$ can be written as $p_{\mathbf{U}}(\mathbf{u}) \propto \exp\left(-\frac{1}{2}\mathbf{u}^\mathsf{T}\mathbf{G}\mathbf{u}\right)$ with the positive definite matrix $\mathbf{G} \triangleq \varepsilon^2 \mathbb{1}_{n\times n} + \mathbf{H}^\mathsf{T}\mathbf{H}$, where $\mathbb{1}_{n\times n}$ is the $n \times n$ identity matrix. Then, $p_{\mathbf{U}_\mathcal{S}|\mathbf{U}_{\bar{\mathcal{S}}}}(\mathbf{u}_\mathcal{S}|\mathbf{u}_{\bar{\mathcal{S}}}) \propto \exp\left(-\frac{1}{2}\mathbf{u}_\mathcal{S}^\mathsf{T}\mathbf{G}_{\mathcal{S}|\bar{\mathcal{S}}}\mathbf{u}_\mathcal{S} + \mathbf{n}^\mathsf{T}_{\mathcal{S}|\bar{\mathcal{S}}}\mathbf{u}_\mathcal{S}\right)$, with the positive definite matrix $\mathbf{G}_{\mathcal{S}|\bar{\mathcal{S}}} \triangleq \varepsilon^2 \mathbb{1}_{(m+1)\times(m+1)} + \mathbf{H}_\mathcal{S}^\mathsf{T}\mathbf{H}_\mathcal{S}$ and with $\mathbf{n}_{\mathcal{S}|\bar{\mathcal{S}}}$ being a linear function of $\mathbf{u}_{\bar{\mathcal{S}}}$. The inverse matrix of $\mathbf{G}_{\mathcal{S}|\bar{\mathcal{S}}}$ is the covariance matrix $\mathbf{R}_{\mathcal{S}|\bar{\mathcal{S}}}$ of $\mathbf{U}_\mathcal{S}$ given $\mathbf{U}_{\bar{\mathcal{S}}}$. For $i \in \mathcal{S}$, a well-known property of jointly Gaussian random variables says that the i-th diagonal entry of $\mathbf{R}_{\mathcal{S}|\bar{\mathcal{S}}}$ equals $\sigma^2_{i|\bar{\mathcal{S}}}(\varepsilon)$.

Without loss of generality, we can assume that $\mathcal{S} = \{0, 1, \ldots, m\}$ and that $i = 0$. Because $\mathbf{H}_\mathcal{S} = \left(\mathbf{H}_{\{0\}} | \mathbf{H}_{\mathcal{S}\setminus 0}\right)$, we obtain

$$\mathbf{G}_{\mathcal{S}|\bar{\mathcal{S}}} \triangleq \left[\begin{array}{c|c} \varepsilon^2 \mathbb{1}_{1\times 1} + \mathbf{H}^\mathsf{T}_{\{0\}}\mathbf{H}_{\{0\}} & \mathbf{H}^\mathsf{T}_{\{0\}}\mathbf{H}_{\mathcal{S}\setminus 0} \\ \hline \mathbf{H}^\mathsf{T}_{\mathcal{S}\setminus 0}\mathbf{H}_{\{0\}} & \varepsilon^2 \mathbb{1}_{m\times m} + \mathbf{H}^\mathsf{T}_{\mathcal{S}\setminus 0}\mathbf{H}_{\mathcal{S}\setminus 0} \end{array}\right].$$

Since $\sigma^2_{0|\bar{\mathcal{S}}}(\varepsilon)$ is the $(0,0)$-entry of $\mathbf{R}_{\mathcal{S}|\bar{\mathcal{S}}} = \mathbf{G}^{-1}_{\mathcal{S}|\bar{\mathcal{S}}}$, we have

$$\sigma^2_{0|\bar{\mathcal{S}}}(\varepsilon) = \gamma^{-2}_{\mathcal{S}|\bar{\mathcal{S}}}(\varepsilon) \cdot \det\left(\varepsilon^2 \mathbb{1}_{m\times m} + \mathbf{H}^\mathsf{T}_{\mathcal{S}\setminus 0}\mathbf{H}_{\mathcal{S}\setminus 0}\right),$$

where $\gamma_{\mathcal{S}|\bar{\mathcal{S}}}(\varepsilon) \triangleq \sqrt{\det\left(\mathbf{G}_{\mathcal{S}|\bar{\mathcal{S}}}\right)}$. In the limit $\varepsilon \to 0$ we have

$$\begin{aligned}\lim_{\varepsilon \to 0} \det\left(\varepsilon^2 \mathbb{1}_{m\times m} + \mathbf{H}^\mathsf{T}_{\mathcal{S}\setminus 0}\mathbf{H}_{\mathcal{S}\setminus 0}\right) &= \det{}_\mathbb{Z}\left(\mathbf{H}^\mathsf{T}_{\mathcal{S}\setminus 0}\mathbf{H}_{\mathcal{S}\setminus 0}\right) \\ &= \det{}_\mathbb{Z}\left(\mathbf{H}^\mathsf{T}_{\mathcal{S}\setminus 0}\right) \cdot \det{}_\mathbb{Z}\left(\mathbf{H}_{\mathcal{S}\setminus 0}\right) = \det{}_\mathbb{Z}\left(\mathbf{H}_{\mathcal{S}\setminus 0}\right)^2 \overset{(*)}{=} \omega_0^2,\end{aligned}$$

where step $(*)$ follows from Definition 4. Similar expressions easily follow for other $i \in \mathcal{S}$, therefore proving (11). ■

Remark 20 Remember that the differential entropy of an n-dimensional Gaussian random vector $\mathbf{U}$ with mean vector $\mathbf{m}$ and covariance matrix $\mathbf{R}$ is $h(\mathbf{U}) = \frac{1}{2}\log\left((2\pi\,\mathrm{e})^n \det(\mathbf{R})\right)$ (in nats) [9]. Therefore, the result of Theorem 19 can also be expressed as

$$\omega_i = \lim_{\varepsilon \to 0} \gamma'_{\mathcal{S}|\bar{\mathcal{S}}}(\varepsilon) \cdot \exp\left(h\left(U_i | \mathbf{U}_{\bar{\mathcal{S}}}\right)\right)$$

for all $i \in \mathcal{I}$, where $\gamma'_{\mathcal{S}|\bar{\mathcal{S}}}(\varepsilon) \triangleq \frac{1}{\sqrt{2\pi\,\mathrm{e}}}\gamma_{\mathcal{S}|\bar{\mathcal{S}}}(\varepsilon)$. □

Remark 21 One can associate an electrical network to the Gaussian graphical model in Theorem 19 [10], [11]. Theorem 19 can then be seen as relating ω_i to the square root of a certain effective (or input) resistance of some suitably defined electrical network [12] whose topology equals the topology of $\mathsf{T}(\mathbf{H})$. □

VI. Conclusions

In this paper we have introduced the concept of absdet-pseudo-codewords and perm-pseudo-codewords towards a better understanding of the fundamental cone of a parity-check matrix. We have shown that these vectors are in the fundamental cone and that it is therefore justified to call them absdet-pseudo-codewords and perm-pseudo-codewords. We have discussed some simple examples that show the relevance of these pseudo-codewords and we have highlighted some of their properties. There are many interesting avenues for further research of these pseudo-codewords. In particular, it promises to be worthwhile to relate them to the statements about matchings in [13], and to potentially combine them with the pseudo-codeword search algorithm in [14].

References

[1] D. J. C. MacKay and M. C. Davey, "Evaluation of Gallager codes for short block length and high rate applications," in *Codes, Systems, and Graphical Models (Minneapolis, MN, 1999)*, B. Marcus and J. Rosenthal, Eds. Springer Verlag, New York, Inc., 2001, pp. 113–130.

[2] R. Smarandache and P. O. Vontobel, "On regular quasi-cyclic LDPC codes from binomials," in *Proc. IEEE Int. Symp. Information Theory*, Chicago, IL, USA, June 27–July 2 2004, p. 274.

[3] ——, "Quasi-cyclic LDPC codes: influence of proto- and Tanner-graph structure on minimum Hamming distance upper bounds," *submitted to IEEE Trans. Inf. Theory, available online under* `http://arxiv.org/abs/0901.4129`, Jan. 2009.

[4] J. Feldman, "Decoding error-correcting codes via linear programming," Ph.D. dissertation, Massachusetts Institute of Technology, Cambridge, MA, 2003.

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

[6] R. Koetter and P. O. Vontobel, "Graph covers and iterative decoding of finite-length codes," in *Proc. 3rd Intern. Symp. on Turbo Codes and Related Topics*, Brest, France, Sept. 1–5 2003, pp. 75–82.

[7] 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, available online under* `http://www.arxiv.org/abs/cs.IT/0512078`, 2007.

[8] R. Koetter, W.-C. W. Li, P. O. Vontobel, and J. L. Walker, "Characterizations of pseudo-codewords of (low-density) parity-check codes," *Adv. in Math.*, vol. 213, no. 1, pp. 205–229, Aug. 2007.

[9] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, ser. Wiley Series in Telecommunications. New York: John Wiley & Sons Inc., 1991, a Wiley-Interscience Publication.

[10] J. B. Dennis, *Mathematical Programming and Electrical Networks*. The Technology Press of The Massachusetts Institute of Technology, Cambridge, MA, 1959.

[11] P. O. Vontobel, *Kalman Filters, Factor Graphs, and Electrical Networks*. Post-Diploma Project, ETH Zurich, 2002.

[12] ——, "Factor graphs, electrical networks, and entropy," in *Proc. 40th Allerton Conf. on Communication, Control, and Computing*, Allerton House, Monticello, Illinois, USA, Oct. 2–4 2002.

[13] M. Chertkov, V. Y. Chernyak, and R. Teodorescu, "Belief propagation and loop series on planar graphs," *J. Stat. Mech.: Theory and Experiment*, P05003, 2008.

[14] M. Chertkov and M. G. Stepanov, "An efficient pseudocodeword search algorithm for linear programming decoding of LDPC codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 4, pp. 1514–1520, Apr. 2008.