On Minimal Pseudo-Codewords

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

***Abstract*—The performance of linear-programming decoding of a binary linear code described by a parity-check matrix depends on the set of pseudo-codewords associated to this matrix and in particular, on the set of minimal pseudo-codewords.**

This paper attempts to provide an algebraic characterization of the minimal pseudo-codewords. It also provides a connection between the fundamental cone of a Tanner graph and the fundamental cone of its Forney-style factor graph.

***Index Terms*—Fundamental cone, linear-programming decoding, low-density parity-check code, pseudo-codewords.**

I. Introduction

Linear-programming (LP) decoding has emerged as an interesting approach to decoding binary linear codes [1], [2]. The present paper attempts to present a characterization of the set of pseudo-codewords and, in particular, of the set of minimal pseudo-codewords, the objects which determine the performance of an LP decoder.

The main focus of the present paper is the derivation of certain results on the structure of minimal pseudo-codewords. Such results are immediately relevant to LP decoding. Additionally, through the intuitive connection made by Koetter and Vontobel [3], [4] between message-passing iterative (MPI) decoding and LP decoding, these results have implications for MPI decoding as well.[1] In addition, these results have relevance also to compressed sensing through the connection made in [5], [6] between channel coding LP decoding and compressed sensing LP decoding.

In [7], the authors introduce two classes of pseudo-codewords, called absdet-pseudo-codewords and perm-pseudo-codewords, which seem to be important in the characterization of the performance of LP decoding and MPI decoding. In this paper we develop further on their importance relative to a subclass of pseudo-codewords which we call pseudo-codewords *of the nullspace type*. These are pseudo-codewords associated with vectors in the $\mathbb{Z}$-nullspace of the parity-check matrix. We show that minimal pseudo-codewords of the nullspace type can be found only among the absdet-pseudo-codewords. In addition, the absdet-pseudo-codewords constitute a "basis" for the set of all pseudo-codewords of the nullspace type, i.e., any pseudo-codeword of the nullspace type is associated to a vector in the $\mathbb{Z}$-nullspace of the parity-check matrix; this vector is a linear combination of the vectors in the $\mathbb{Z}$-nullspace that are associated to the absdet-pseudo-codewords. We obtain thus a complete characterization of the minimal pseudo-codewords of the nullspace type. We will also discuss the case of pseudo-codewords that are not of the nullspace type.

The remainder of the paper is structured as follows. In Section II we list basic notations and definitions. In Section III we give a bound on the support of all minimal pseudo-codewords. Based on this bound, in Section IV we build further on the importance of the absdet-pseudo-codewords and give a complete characterization of the minimal pseudo-codewords of the nullspace type. In Section V we attempt a characterization of the remaining minimal pseudo-codewords. Section VI looks at the pseudo-codewords through the known map between a Tanner graph $\mathcal{G}$ and its Forney factor graph $\mathcal{G}'$; of particular interest is the way that the absdet-pseudo-codewords and perm-pseudo-codewords are affected by that map. We conclude the paper in Section VII.

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 $\mathbf{M}$ 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 submatrix 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 write $\mathbf{M}_{\mathcal{S}}$ instead of $\mathbf{M}_{\mathcal{R},\mathcal{S}}$; and we will use $\mathcal{S} \setminus i$ for $\mathcal{S} \setminus \{i\}$.

Let $\mathbf{H} = (h_{j,i}) \in \mathbb{F}_2^{m \times n}$ 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 $\mathbf{H}$, and $\mathcal{I}_j(\mathbf{H}) \triangleq \{i \in \mathcal{I} \mid h_{j,i} = 1\}$.

We review the following important definitions.

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

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

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

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

[1] In particular, in all the cases where an exact characterization of the min-sum algorithm is possible, block-wise graph-cover decoding gives also the correct predictions, and in all the cases where an exact characterization of the sum-product algorithm is possible, symbol-wise graph-cover decoding gives also the correct predictions.

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

then $\boldsymbol{\omega}$ is called an unscaled pseudo-codeword. (For a motivation of these definitions, see [3]).

As mentioned in [3], minimal pseudo-codewords in $\mathcal{K}(\mathbf{H})$ completely characterize the region in the log-likelihood ratio vector space where LP decoding decides for the all-zero codeword; the knowledge of non-minimal pseudo-codewords is however also valuable since such pseudo-codewords can be used to bound this decision region.

In [7], the notions of det-vectors, absdet-pseudo-codewords, and perm-pseudo-codewords were introduced. We briefly review these definitions.

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

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

where $\eta_{\mathcal{S}}(i) \in \{0, 1, \ldots, |\mathcal{S}|-1\}$ is the index of i within the set $\mathcal{S}$ and $\det_{\mathbb{Z}}(\cdot)$ is the $\mathbb{Z}$-determinant operator. The *absdet-vector* based on $\mathcal{S}$ is the vector $\boldsymbol{\omega} \in \mathbb{Z}^n$ with components

$$\omega_i \triangleq \begin{cases} \Big|\det_{\mathbb{Z}}\big(\mathbf{H}_{\mathcal{S}\setminus i}\big)\Big| & \text{if } i \in \mathcal{S} \\ 0 & \text{otherwise} \end{cases},$$

i.e., the components of the absdet-vectors are the absolute value of the components of the det-vector. Finally, the *perm-vector* based on $\mathcal{S}$ is the vector $\boldsymbol{\omega} \in \mathbb{Z}^n$ with components

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

where $\mathrm{perm}_{\mathbb{Z}}(\cdot)$ denotes the $\mathbb{Z}$-permanent operator.

We remind the following lemma from [7].

Lemma 1 *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 $\mathbf{H}\cdot\boldsymbol{\nu}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$ in $\mathbb{R}$. Then the vector $\boldsymbol{\omega} \in \mathbb{R}^n$ with components $\omega_i \triangleq |\nu_i|$, $i \in \mathcal{I}$, satisfies $\boldsymbol{\omega} \in \mathcal{K}(\mathbf{H})$.*

For convenience, we will extend the absolute value notation from complex numbers to vectors and write $\boldsymbol{\omega} = |\boldsymbol{\nu}|$ for a vector satisfying the conditions of Lemma 1 and say that such an $\boldsymbol{\omega}$ is a pseudo-codeword *of the nullspace type*. Since the det-vector $\boldsymbol{\nu}$ based on $\mathcal{S}$ satisfies $\mathbf{H}\cdot\boldsymbol{\nu}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$ in $\mathbb{Z}$ we obtain that the absdet-vector $\boldsymbol{\omega}$ based on $\mathcal{S}$ is an unscaled pseudo-codeword of $\mathbf{H}$ of the nullspace type. In [7], it was shown that the perm-vectors are also unscaled pseudo-codewords. We will see that they are not necessarily of the nullspace type.

III. Bound on the Size of the Support of a Minimal Pseudo-codeword

The following theorem gives an upper bound on the size of the support of any minimal pseudo-codeword. This bound will be used in identifying all the minimal pseudo-codewords of the nullspace type.[2]

[2]Results equivalent to the ones in this section were also derived in [8] using a different approach.

Theorem 2 *If $\mathcal{C}$ is a binary linear code described by a parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{m\times n}$, $m \leqslant n$, and $\boldsymbol{\omega}$ is a minimal pseudo-codeword for $\mathbf{H}$, then*

$$|\operatorname{supp}(\boldsymbol{\omega})| \leqslant m+1. \tag{3}$$

If $\boldsymbol{\omega}$ is a minimal pseudo-codeword of the nullspace type, then

$$|\operatorname{supp}(\boldsymbol{\omega})| \leqslant \operatorname{rank}_{\mathbb{R}}(\mathbf{H}) + 1 \leqslant m+1. \tag{4}$$

Proof: Let $\mathbf{A}$ be the $k\times n$ matrix of rank $n-1$, $k \geqslant n-1$, obtained from the inequalities (1) and (2) that are satisfied with equality. Then $\mathbf{A}\cdot\boldsymbol{\omega}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$ in $\mathbb{R}$.

Let $|\operatorname{supp}(\boldsymbol{\omega})| = l$. For convenience and without loss of generality, we suppose that the first l positions of $\boldsymbol{\omega}$ are nonzero; otherwise, we use column operations on $\mathbf{A}$ to bring the columns corresponding to the support of $\boldsymbol{\omega}$ to the first l positions. Appropriately interchanging rows, we can rearrange the matrix $\mathbf{A}$ to have the form $\mathbf{A} = \begin{bmatrix} \mathbf{M} & \mathbf{N} \\ \mathbf{0} & \mathbf{I}_{n-l} \end{bmatrix}$. In addition, we can assume that each row of $\mathbf{H}$ is represented in $\mathbf{M}$ at most once by an inequality as in (2). Indeed, if one row would have two associated rows in $\mathbf{M}$, then we would have a submatrix of $\mathbf{M}$ of the form $\begin{bmatrix} -1 & 1 & 1 & 1 & \ldots & 0 & 0 & \ldots \\ 1 & -1 & 1 & 1 & \ldots & 0 & 0 & \ldots \end{bmatrix}$, which has kernel non-negative vectors with a zero component on the positions of the support of $\boldsymbol{\omega}$, an impossible situation; and if the submatrix is $\begin{bmatrix} -1 & 1 & 0 & 0 & \ldots \\ 1 & -1 & 0 & 0 & \ldots \end{bmatrix}$ then the second row does not contribute to the rank of $\mathbf{A}$ and it can be discarded.

Appropriately subtracting multiples of some of the last $n-l$ rows from some of the rows corresponding to the matrix $\mathbf{N}$, we can reduce the matrix to

$$\mathbf{A} = \begin{bmatrix} \mathbf{M} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{n-l} \end{bmatrix}. \tag{5}$$

The rank of $\mathbf{A}$ can then be easily computed as

$$n-1 = \operatorname{rank}_{\mathbb{R}}(\mathbf{A}) = n - l + \operatorname{rank}_{\mathbb{R}}(\mathbf{M}), \tag{6}$$

from which $\operatorname{rank}_{\mathbb{R}}(\mathbf{M}) = l-1 = |\operatorname{supp}(\boldsymbol{\omega})| - 1$ and since $\operatorname{rank}_{\mathbb{R}}(\mathbf{M}) \leqslant m+1$ we obtain $|\operatorname{supp}(\boldsymbol{\omega})| \leqslant m+1$.

If $\boldsymbol{\omega}$ is of the nullspace type, then let $\boldsymbol{\nu} \in \mathbb{R}^n$ such that $\boldsymbol{\omega} = |\boldsymbol{\nu}|$ and $\mathbf{H}\cdot\boldsymbol{\nu}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$ in $\mathbb{R}$. Changing the sign of the ith column of $\mathbf{H}$ if $\nu_i < 0$, we obtain a submatrix $\mathbf{M}'$ of $\mathbf{A}$ coresponding to inequalities (2), which can be further reduced as above to give $\mathbf{M}$. Since $\operatorname{rank}(\mathbf{M}) \leqslant \operatorname{rank}(\mathbf{M}') = \operatorname{rank}(\mathbf{H})$ we obtain the claim. ∎

Remark 3 From the above proof we see that we can assume that $\mathbf{A}$ has the representation given by (5) after a permutation of the components of $\boldsymbol{\omega}$ so that the nonzero components are on the first $l = |\operatorname{supp}(\boldsymbol{\omega})|$ positions. In addition, we can take the matrix $\mathbf{M}$ above to have full rank, equal to $l-1$ according to (6). Therefore a matrix $\mathbf{M}$ of minimal size can be obtained from an $(l-1)\times l$ submatrix of $\mathbf{H}$ with columns indexed by the support $\operatorname{supp}(\boldsymbol{\omega}) \triangleq \{i_1, \ldots, i_l\}$ of $\boldsymbol{\omega}$, such that on each of the rows one of the entries is changed from 1 into -1, giving $\mathbf{M}\cdot(\omega_{i_1}, \ldots, \omega_{i_l})^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$ in $\mathbb{R}$. We state this fact in the following lemma. □

Lemma 4 *Let $\mathcal{C}$ be a binary linear code described by a parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{m\times n}$ and let $\boldsymbol{\omega}$ be a* minimal *pseudo-codeword for $\mathbf{H}$ with $\mathrm{supp}(\boldsymbol{\omega}) = \{i_1, \ldots, i_l\}$.*

Then there exists a full rank $(l-1)\times l$ submatrix of $\mathbf{H}$ with columns indexed by the support of $\boldsymbol{\omega}$ for which it is possible to change on each of its rows one of the entries of 1 into -1 to obtain a full rank $(l-1)\times l$ matrix $\mathbf{M}$ such that $\mathbf{M}\cdot(\omega_{i_1},\ldots,\omega_{i_l})^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$ (in $\mathbb{R}$).

Moreover, if $\mathbf{A}$ denotes the matrix of rank $n-1$ associated to the inequalities of the fundamental cone that are satisfied with equality, then the system describing the minimal pseudo-codeword $\mathbf{A}\cdot\boldsymbol{\omega}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$ (in $\mathbb{R}$) is equivalent to the following system

$$\mathbf{M}\cdot(\omega_{i_1},\ldots,\omega_{i_l})^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}} \quad \textit{(in } \mathbb{R}) \qquad (7)$$
$$\omega_i = 0, \text{ for all } i \in \mathcal{I}(\mathbf{H}) \setminus \{i_1,\ldots,i_l\}.$$

IV. Minimal pseudo-codewords of the nullspace type

The pseudo-codewords of the null-space type are of interest because of the recent connections that were established between channel coding LP decoding and compressed sensing LP decoding [5], [6]. The main ingredient in these connections is Lemma 1 which maps vectors in the nullspace of some zero-one matrix (called a *measurement matrix* in compressed sensing) to vectors of the fundamental cone defined by that matrix. This allows performance guaranties when using a good parity-check matrix for LP in compressed sensing.

A relevant question in this connection is when a nonzero vector in the null-space of a measurement matrix is mapped, through the absolute value mapping of Lemma 1, to a minimal pseudo-codeword. This section provides the answer.

Suppose $\mathbf{H}$ has full rank m over $\mathbb{R}$ and suppose for convenience, without loss of generality, that the first m columns are $\mathbb{R}$-linearly independent. The following theorem shows a simple fact about the set of det-vectors $\{\boldsymbol{\nu}_i\}_{i\in\{m,\ldots,n-1\}}$ based on the size $m+1$ set $\mathcal{S}_i \triangleq \{0,1,\ldots,m-1,i\}$. Namely, it shows that this set of $n-m$ vectors forms a basis over $\mathbb{Z}$ for the set of all solutions of the system $\mathbf{H}\cdot\boldsymbol{\nu}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$ over $\mathbb{Z}$. Applying now Lemma 1, we obtain that the absdet-pseudo-codewords "span" the subset of pseudo-codewords of the nullspace type. This means that any pseudo-codeword $\boldsymbol{\omega}$ obtained from a vector $\boldsymbol{\nu}\in\mathbb{Z}^n$ in the nullspace of $\mathbf{H}$, i.e., $\mathbf{H}\cdot\boldsymbol{\nu}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$ over $\mathbb{Z}$, by the absolute value mapping, i.e., $\boldsymbol{\omega} = |\boldsymbol{\nu}|$, has the property that there exist $a_i\in\mathbb{Z}$, $m\leqslant i\leqslant n-1$, such that $\boldsymbol{\omega} = \left|\sum_{i=m}^{n-1} a_i\boldsymbol{\nu}_i\right|$. In addition, after proper scaling, the set of vectors $\{\boldsymbol{\nu}_i \bmod 2\}_{m\leqslant i\leqslant n-1}$ forms a basis for the set of codewords in $\mathcal{C}$, giving a generator matrix.

We state this result in a more general form.

Theorem 5 *Let $\mathcal{C}$ be a binary linear code described by the parity-check matrix $\mathbf{H}\in\mathbb{F}_2^{m\times n}$, $(m<n)$ of rank $m'\leqslant m$ over $\mathbb{R}$, and let $\mathbf{H}'$ be an $m'\times n$ submatrix of $\mathbf{H}$ of full rank. Let $\mathcal{S} = \{i_1,i_2,\ldots,i_{m'}\}\subset\mathcal{I}(\mathbf{H}')$ be a set of m' $\mathbb{Z}$-linearly independent columns of $\mathbf{H}'$. For each $i\in\mathcal{I}(\mathbf{H}')\setminus\mathcal{S}$, let $\mathcal{S}_i = \mathcal{S}\cup\{i\}$ and let $\boldsymbol{\nu}_i$ be the det-vector of $\mathbf{H}'$ based on $\mathcal{S}_i$. Then the set $\{\boldsymbol{\nu}_i\}_{i\in\mathcal{I}(\mathbf{H}')\setminus\mathcal{S}}$ forms a basis over the integers for the set of solutions of the real system*

$$\mathbf{H}\cdot\boldsymbol{\nu}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}} \quad \textit{(in } \mathbb{Z}). \qquad (8)$$

Moreover, if we assume that $\mathbf{H}$ has rank m' also over $\mathbb{F}_2$ and that $\boldsymbol{\nu}_i$ is scaled such that the vector $\boldsymbol{\nu}_i \bmod 2 \neq 0$, then the set $\{\boldsymbol{\nu}_i \bmod 2\}_{i\in\mathcal{I}(\mathbf{H}')\setminus\mathcal{S}}$ forms a basis for the set of codewords in $\mathcal{C}$. Finally, any pseudo-codeword $\boldsymbol{\omega}$ for which there is a vector $\boldsymbol{\nu}\in\mathbb{Z}^n$ such that $\mathbf{H}\cdot\boldsymbol{\nu}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$ over $\mathbb{Z}$ and such that $\boldsymbol{\omega} = |\boldsymbol{\nu}|$, has the property that there exist $a_i\in\mathbb{Z}, i\in\mathcal{I}(\mathbf{H})\setminus\mathcal{S}$ such that $\boldsymbol{\omega} = \left|\sum_{i\in\mathcal{I}(\mathbf{H})\setminus\mathcal{S}} a_i\boldsymbol{\nu}_i\right|$.

Proof: The set of solutions of $\mathbf{H}\cdot\boldsymbol{\nu}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$ is a subspace of $\mathbb{R}^n$ of dimension $n-m'$. Note that the set of det-vectors $\{\boldsymbol{\nu}_i\}_{i\in\mathcal{I}(\mathbf{H}')\setminus\mathcal{S}}$ has at least $n-m'-1$ zero components on the positions $j\notin\mathcal{S}_i$. The remaining components on the positions $j\in\mathcal{S}_i$ equal to certain subdeterminants of $\mathbf{H}'$. Moreover, the ith-component of each det-vector $\boldsymbol{\nu}_i$ is nonzero, equal to $\det(\mathbf{H}'_{\mathcal{S}})$. Therefore, they form exactly $n-m'$ linearly independent solutions of the system (8). Taking the system modulo 2 and applying the same argument, we obtain the claim regarding the basis for the set of codewords. ■

The choice of $\mathcal{S}$ might not be unique; each m $\mathbb{R}$-linearly independent columns of $\mathbf{H}$ will give a different basis of det-vectors. An integer solution can then be obtained by taking $\mathbb{Z}$-linear combinations of a chosen set of det-vectors.

Example 6 Let $\mathcal{C}$ be a $[4,2,2]$ binary linear code based on the parity-check matrix $\mathbf{H}\triangleq\begin{bmatrix}1&1&1&0\\0&1&1&1\end{bmatrix}$. Let $\mathcal{S}=\{0,1\}$. Then the sets $\mathcal{S}_i = \mathcal{S}\cup\{i\}$ are $\mathcal{S}_2 = \{0,1,2\}$ and $\mathcal{S}_3 = \{0,1,3\}$. The absdet-pseudo-codewords corresponding to these sets are: $(0,1,1,0)$ and $(1,1,0,1)$ which are equal to their modulo 2 projections. The codewords form a generator matrix for the code. Over $\mathbb{Z}$, they form a generator matrix for the set of solutions of $\mathbf{H}\cdot\boldsymbol{\nu}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$ in $\mathbb{Z}$.

Taking $\mathcal{S} = \{2,3\}$, and $\mathcal{S}_0 = \{0,2,3\}$ and $\mathcal{S}_1 = \{1,2,3\}$, we obtain the absdet-pseudo-codewords $(1,0,1,1)$ and $(0,1,1,0)$, which are equal to their modulo 2 projections. The two codewords form another generator matrix. □

We are now ready to answer our initial question: when is a pseudo-codeword $\boldsymbol{\omega}$ of the nullspace type minimal? The answer is given in the following theorem: only when it is an absdet-pseudo-codeword of $\mathbf{H}$ or an absdet-pseudo-codeword of a submatrix of $\mathbf{H}$ if the absdet-pseudo-codeword based on a set $\mathcal{S}$ of $m+1$ elements containing the support of $\boldsymbol{\omega}$ is zero (when $\mathbf{H}_{\mathcal{S}}$ is not full rank). The reverse is not true; we omit to give a counterexample due to space constraints.

Theorem 7 *Let $\mathcal{C}$ be a binary linear code described by an $m\times n$, $(m<n)$ parity-check matrix $\mathbf{H}$, and let $\boldsymbol{\omega}$ be a minimal pseudo-codeword of the nullspace type. Let $\mathcal{S}\triangleq\mathrm{supp}(\boldsymbol{\omega})\triangleq\{i_1,i_2,\ldots,i_l\}$. Then there exists a set $\mathcal{T}\subset\mathcal{J}(\mathbf{H}_{\mathcal{S}})$ of $l-1$ $\mathbb{Z}$-linearly independent rows of $\mathbf{H}_{\mathcal{S}}$ such that $\boldsymbol{\omega}$ is an absdet-pseudo-codeword of the matrix $\mathbf{H}_{\mathcal{T},\mathcal{I}(\mathbf{H})}$ based on $\mathcal{S}$.*

Proof: From Lemma 2 we have $l \leqslant \mathrm{rank}_{\mathbb{R}}(\mathbf{H}) + 1$. Let $\boldsymbol{\nu} \in \mathbb{R}^n$ such that $\boldsymbol{\omega} = |\boldsymbol{\nu}|$ and $\mathbf{H} \cdot \boldsymbol{\nu}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$ in $\mathbb{R}$. Then $\mathbf{H}_{\mathcal{S}} \cdot \boldsymbol{\nu}_{\mathcal{S}}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$ and $\boldsymbol{\omega}_{\mathcal{S}} = |\boldsymbol{\nu}_{\mathcal{S}}|$, so $\boldsymbol{\omega}_{\mathcal{S}}$ is a pseudo-codeword for $\mathbf{H}_{\mathcal{S}}$ of the nullspace type. We also have that the matrix $\mathbf{M}$ in the representation of Lemma 4 must correspond to a submatrix of $\mathbf{H}_{\mathcal{S}}$ of rank $l-1$. Therefore, $\boldsymbol{\omega}_{\mathcal{S}}$ is a minimal pseudo-codeword for $\mathbf{H}_{\mathcal{S}}$ and necessarily $\mathrm{rank}(\mathbf{H}_{\mathcal{S}}) = l - 1$. Let $\mathcal{T} \subset \mathcal{J}(\mathbf{H})$ be a set of $l-1$ $\mathbb{Z}$-linearly independent rows of $\mathbf{H}_{\mathcal{S}}$, let $\boldsymbol{\mu}_{\mathcal{S}} \in \mathbb{Z}^l$ denote the det-vector of $\mathbf{H}_{\mathcal{T},\mathcal{S}}$ based on $\mathcal{S}$ and let $\boldsymbol{\mu} \in Z^n$ be its length-n extension obtained by adding zero components on the positions $i \notin \mathcal{S}$. According to Theorem 5, $\boldsymbol{\mu}_{\mathcal{S}}$ gives a basis over the integers for the set of solutions of $\mathbf{H}_{\mathcal{S}} \cdot \boldsymbol{\nu}_{\mathcal{S}}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$ (in $\mathbb{Z}$). Then there exists $a \in \mathbb{Z}$, such that $\boldsymbol{\nu}_{\mathcal{S}} = a\boldsymbol{\mu}_{\mathcal{S}}$. It implies that, up to scaling by a, the two vectors are equal resulting in $\boldsymbol{\omega} = a\boldsymbol{\mu}$. Since $\boldsymbol{\mu}$ is an absdet-pseudo-codeword for $\mathbf{H}_{\mathcal{T},\mathcal{I}(\mathbf{H})}$, the claim follows. ∎

The following theorem gives a family of matrices for which the absdet-pseudo-codewords are always minimal.

Theorem 8 *Let $\mathcal{C}$ be a binary linear code described by a parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{m \times n}$, $m < n$. Let $\mathcal{S}$ be a size-$(m+1)$ subset of $\mathcal{I}(\mathbf{H})$, let $m' \triangleq \mathrm{rank}_{\mathbb{R}}(\mathbf{H}_{\mathcal{S}})$, and let $\mathbf{H}' \subset \mathbf{H}_{\mathcal{S}}$ be an $m' \times (m'+1)$ matrix of full rank. Let $\boldsymbol{\omega} \in \mathbb{Z}^{m'+1}$ be the absdet-pseudo-codeword of $\mathbf{H}'$ based on $\mathcal{I}(\mathbf{H}')$ and define $\bar{\boldsymbol{\omega}} \in \mathbb{Z}^n$ to be its natural n-extension*

$$\bar{\omega}_i \triangleq \begin{cases} \omega_i & \text{if } i \in \mathcal{I}(\mathbf{H}') \\ 0 & \text{otherwise} \end{cases} .$$

Suppose that $\mathbf{H}'$ has row degree at most 3, then $\bar{\boldsymbol{\omega}}$ is a minimal pseudo-codeword for $\mathbf{H}$.

Proof: Let $\boldsymbol{\nu} = (\nu_i) \in \mathbb{Z}^{m'+1}$ such that $\mathbf{H}' \cdot \boldsymbol{\nu}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$ in $\mathbb{Z}$ and $\boldsymbol{\omega} = |\boldsymbol{\nu}|$. Let $\mathbf{M}'$ be the $m' \times (m'+1)$ matrix such that

$$\mathrm{col}_i(\mathbf{M}') \triangleq \begin{cases} -\mathrm{col}_i(\mathbf{H}') & \text{if } \nu_i < 0 \\ \mathrm{col}_i(\mathbf{H}') & \text{if } \nu_i \geqslant 0 \end{cases} ,$$

where $\mathrm{col}_i(\mathbf{M}')$ and $\mathrm{col}_i(\mathbf{H}')$ denote the ith column of $\mathbf{M}'$ and $\mathbf{H}'$, respectively. Then $\mathbf{M}' \cdot \boldsymbol{\omega}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$ in $\mathbb{Z}$. Since the row degree of $\mathbf{H}'$ is at most 3, each equation in $\mathbf{H}' \cdot \boldsymbol{\nu}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$ involves at most 3 variables. Therefore, changes of signs must occur in the nonzero components ν_i that participate in that equation: if the equation involves three nonzero components then two must have the same sign and one not; if there are only two nonzero components involved in the equation, then they must be equal in their absolute value and of different sign. Therefore each row of $\mathbf{M}'$ must be nonzero (since $\mathbf{M}'$ is full rank) and must contain either only one negative entry or only one positive entry. Therefore, $\mathbf{M}'$ is a submatrix of the matrix $\mathbf{A}'$ describing the inequalities of the fundamental cone that are satisfied with equality. Since $\mathrm{rank}_{\mathbb{R}}(\mathbf{H}') = \mathrm{rank}_{\mathbb{R}}(\mathbf{M}') = m'$, we obtain, together with $n - (m'+1)$ equations $\bar{\omega}_i = 0$ for all $i \notin \mathcal{I}(\mathbf{H}')$, that $\bar{\boldsymbol{\omega}}$ is minimal for $\mathbf{H}$. ∎

V. Minimal pseudo-codewords not of the nullspace type

The minimal pseudo-codewords that are not of the nullspace type are unfortunately not (yet) as compactly described. What we can say so far about the behavior of these pseudo-codewords is the following.

Let $\boldsymbol{\omega}$ be a minimal pseudo-codeword not in the $\mathbb{R}$-nullspace of $\mathbf{H}$, of support size l with $l \leqslant m+1$ (for $m < n$). Then, there does not exist a vector $\boldsymbol{\nu}$ in the $\mathbb{R}$-nullspace of $\mathbf{H}$ such that $|\boldsymbol{\nu}| = \boldsymbol{\omega}$, but there could be two or more $\boldsymbol{\nu}_1, \boldsymbol{\nu}_2, \ldots, \boldsymbol{\nu}_k$ such that $|\boldsymbol{\nu}_i| = \boldsymbol{\omega}$ and each $\boldsymbol{\nu}_i$ is in the nullspace of some $|\mathcal{R}_i| \times n$ submatrix $\mathbf{H}_i$ of $\mathbf{H}$, $|\mathcal{R}_i| < m, i = 1, 2, \ldots, k$. We give an example.

Example 9 Let

$$\mathbf{H} \triangleq \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

and $\boldsymbol{\omega} = (1, 1, 3, 2, 1, 1, 1)$. Let

$\boldsymbol{\nu}_1 \triangleq (1, 1, -3, 2, -1, 1, -1)$, $\boldsymbol{\nu}_2 \triangleq (1, 1, -3, 2, 1, 1, 1)$,

$\boldsymbol{\nu}_3 \triangleq (1, 1, 3, -2, -1, -1, 1)$, $\boldsymbol{\nu}_4 \triangleq (1, 1, -3, -2, 1, -1, 1)$.

They all map in absolute value to $\boldsymbol{\omega}$, so $\boldsymbol{\omega} = |\boldsymbol{\nu}_i|$. We have

$\mathbf{H} \cdot \boldsymbol{\nu}_1^{\mathsf{T}} = (-2, 0, 0, -2, 4, 0)^{\mathsf{T}}$, $\mathbf{H} \cdot \boldsymbol{\nu}_2^{\mathsf{T}} = (0, 0, 4, 0, 4, 2)^{\mathsf{T}}$,

$\mathbf{H} \cdot \boldsymbol{\nu}_3^{\mathsf{T}} = (4, 0, -2, 0, 0, 0)^{\mathsf{T}}$, $\mathbf{H} \cdot \boldsymbol{\nu}_4^{\mathsf{T}} = (0, 6, 0, -4, 0, 0)^{\mathsf{T}}$,

so $\boldsymbol{\omega} = |\boldsymbol{\nu}_i|$ is a pseudo-codeword of the nullspace type for $\mathbf{H}_{\{1,2,5\},\mathcal{I}(\mathbf{H})}, \mathbf{H}_{\{0,1,3\},\mathcal{I}(\mathbf{H})}, \mathbf{H}_{\{1,3,4,5\},\mathcal{I}(\mathbf{H})}$, and $\mathbf{H}_{\{0,2,4,5\},\mathcal{I}(\mathbf{H})}$, respectively. Note that $\boldsymbol{\omega}$ is a minimal pseudo-codeword for $\mathbf{H}$. □

We note that the union of the rows of $\mathbf{H}$ that are considered for $\boldsymbol{\nu}_3$ and $\boldsymbol{\nu}_4$ is $\mathcal{J}(\mathbf{H})$, so we can describe $\boldsymbol{\omega}$ using only these two vectors. We conjecture that all minimal pseudo-codewords that are not of the nullspace type can be described similarly with only two vectors. Unfortunately, there is not more we can say about these pseudo-codewords at this time.

VI. The Associated Factor Graph Perspective

In this last section we ask if new information on pseudo-codewords can be obtained by taking a factor graph perspective. Of particular interest is the behavior of the absdet- and perm-pseudo-codewords under the map between a Tanner graph $\mathcal{G}$ and a to the Forney-style factor graph of $\mathcal{G}$.

To be more explicit, to an LDPC code $\mathcal{C}$ described by an $m \times n$ parity-check matrix $\mathbf{H}$ to which a Tanner graph $\mathcal{G}$ with m check nodes and n variables nodes corresponds, we can associate a Forney-style factor graph (FFG): the variable nodes are associated with the edges of the Tanner graph and the Tanner graph's variable nodes become each a repetition code. There is also the variant where a half-edge is added to every repetition code, however the topology of the resulting factor graphs is the same.

To this new factor graph, we can also associate a matrix $\mathbf{H}'$ and a code $\mathcal{C}'$ whose parity-check code is $\mathbf{H}'$. In general, the number of rows of $\mathbf{H}'$ is equal to $m + \sum_{i=0}^{n-1}(\deg(x_i) - 1)$, where $\deg(x_i)$ equals the degree of the node x_i in the Tanner graph. The number of columns of $\mathbf{H}'$ is equal to the number of edges of the Tanner graph: $\sum_{i=0}^{n-1}\deg(x_i) = n + \sum_{i=0}^{n-1}(\deg(x_i) - 1)$.

Moreover, if the Tanner graph has, e.g., variable nodes $x_0, x_1, x_2, \ldots, x_{n-1}$, of degrees $3, 2, 4, \ldots$, then there exists a bijective mapping between a codeword $(x_0, x_1, x_2, \ldots)$ in $\mathcal{C}$ and $(x_0, x_0, x_0, x_1, x_1, x_2, x_2, x_2, x_2, \ldots)$ in $\mathcal{C}'$ defined by the FFG. Similarly, one can define a new fundamental polytope and cone for the FFG; again there is a bijective mapping between pseudo-codewords in one and the other.

A natural question when analyzing pseudo-codewords for the FFG is if there are one-to-one mappings of absdet-pseudo-codewords and perm-pseudo-codewords from $\mathbf{H}$ to $\mathbf{H}'$?

The answer is no and yes. The following example will provide some intuition.

Example 10 Let

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

The absdet- and perm-pseudo-codewords are: $(1, 1, 0, 1)$ and $(3, 1, 2, 1)$. We have a node x_0 of degree 1, x_1 of degree 3 and x_2 and x_3 of degree 2. The following matrices represent two possible incidence matrices of the Tanner graph defined by the FFG:

$$\mathbf{H}' = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}, \quad \mathbf{H}'' = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

The absdet-pseudo-codeword $(1, 1, 1, 1, 0, 0, 1, 1)$ and perm-pseudo-codeword $(3, 1, 1, 1, 2, 2, 1, 1)$ of $\mathbf{H}'$ map indeed onto $(1, 1, 0, 1)$ and $(3, 1, 2, 1)$, respectively. Matrix $\mathbf{H}''$ has absdet-pseudo-codeword $(1, 1, 1, 1, 2, 2, 1, 1)$ and perm-pseudo-codeword $(3, 1, 1, 1, 2, 2, 1, 1)$. These map onto $(1, 1, 2, 1)$ and $(3, 1, 2, 1)$, respectively. Note that $(1, 1, 2, 1)$ is a new minimal pseudo-codeword for the Tanner graph of $\mathbf{H}$. In this case, we obtain new information through this FFG mapping. □

We can show that the pseudo-codewords of $\mathbf{H}$ obtained by projecting the perm-pseudo-codewords of $\mathbf{H}'$ will be equal to the perm-pseudo-codewords of $\mathbf{H}$. Here is an intuitive explanation: the entries are permanents of square submatrices $\mathbf{M}$ and $\mathbf{M}'$ of $\mathbf{H}$ and $\mathbf{H}'$, respectively, which are sums of all elementary products. There is a one-to-one correspondence between the elementary products in $\mathbf{M}$ and the ones in $\mathbf{M}'$. We omit the proof of this due to space constraint.

This is not the case for the absdet-pseudo-codewords, as Example 10 already suggested. The reason for this is that in computing the determinant entries of the absdet-pseudo-codewords we take the elementary products together with the signature sign, which can result in new pseudo-codewords through the projection.

Theorem 11 *Let $\mathcal{C}$ and $\mathcal{C}'$ be the binary linear codes described by the $m \times n$ parity-check matrix $\mathbf{H}$, and by the matrix $\mathbf{H}'$ associated to the FFG of $\mathbf{H}$, respectively. Let $f : \mathcal{K}(\mathbf{H}') \mapsto \mathcal{K}(\mathbf{H})$ be a natural bijective projection map on the set of pseudo-codewords of the two matrices. If $\mathrm{Perm}(\mathbf{H})$ and $\mathrm{Perm}(\mathbf{H}')$ are the sets of the perm-pseudo-codewords for $\mathbf{H}$, and $\mathbf{H}$, respectively, then $f(\mathrm{Perm}(\mathbf{H}')) = \mathrm{Perm}(\mathbf{H})$.*

VII. Conclusions

In this paper we have provided a complete characterization of minimal pseudo-codewords of the nullspace type using the set of absdet-pseudo-codewords. An important question for future research concerns the impact of these analytical results on the understanding of the overall performance of the LP decoder. Results in this direction can be found in [8] which explores ideas for fast LP decoding of LDPC codes. Results equivalent to the ones in Section III, which were independently derived there using a different approach, prove to be useful towards this goal. In addition, this paper provides bridging tools for the connections with compressed sensing [5], [6].

VIII. Acknowledgement

We would like to thank Pascal O. Vontobel for his valuable comments and for the many fruitful discussions related to the topic, and to the reviewers for their very helpful suggestions.

References

[1] J. Feldman, "Decoding error-correcting codes via linear programming," Ph.D. dissertation, MIT, Cambridge, MA, 2003.

[2] 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.

[3] P. O. Vontobel and R. Koetter, "Graph-cover decoding and finite-length analysis of message-passing iterative decoding of LDPC codes," *submitted to IEEE Trans. Inform. Theory,* http://www.arxiv.org/abs/cs.IT/0512078, Dec. 2005.

[4] ——, "On the relationship between linear programming decoding and min-sum algorithm decoding," in *Proc. Intern. Symp. on Inform. Theory and its Applications (ISITA)*, Parma, Italy, Oct. 10–13 2004, pp. 991–996.

[5] A. G. Dimakis and P. O. Vontobel, "LP decoding meets LP decoding: a connection between channel coding and compressed sensing," in *Proc. 47th Allerton Conf. on Communications, Control, and Computing*, Allerton House, Monticello, Illinois, USA, Sep. 30–Oct. 2 2009.

[6] A. G. Dimakis, R. Smarandache, and P. O. Vontobel, '"Channel coding LP decoding and compressed sensing LP decoding: further connections," in *Proc. 2010 Intern. Zurich Seminar on Communications*, Zurich, Switzerland, Mar. 3–5 2010.

[7] R. Smarandache and P. O. Vontobel, Absdet-pseudo-codewords and perm-pseudo-codewords: definitions and properties," in *Proc. IEEE Int. Symp. Information Theory*, Seoul, Korea, June 28–July 3 2009.

[8] M. H. Taghavi, A. Shokrollahi, and P. H. Siegel, "Efficient implementation of linear programming decoding, "*submitted to IEEE Trans. Inform. Theory,* http://arxiv.org/abs/0902.0657, Dec. 2008.