

# Characterization of Graph-cover Pseudocodewords of Codes over $\mathbb{F}_3$

Vitaly Skachek

Division of Mathematical Sciences, School of Physical and Mathematical Sciences

Nanyang Technological University, 21 Nanyang Link, Singapore 637371

Email: vitaly.skachek@ntu.edu.sg

**Abstract**—Linear-programming pseudocodewords play a pivotal role in our understanding of the linear-programming decoding algorithms. These pseudocodewords are known to be equivalent to the graph-cover pseudocodewords. The latter pseudocodewords, when viewed as points in the multidimensional Euclidean space, lie inside a fundamental cone. This fundamental cone depends on the choice of a parity-check matrix of a code, rather than on the choice of the code itself. The cone does not depend on the channel, over which the code is employed.

The knowledge of the boundaries of the fundamental cone could help in studying various properties of the pseudocodewords, such as their minimum pseudoweight, pseudoredundancy of the codes, etc. For the binary codes, the full characterization of the fundamental cone was derived by Koetter et al. However, if the underlying alphabet is large, such characterization becomes more involved. In this work, a characterization of the fundamental cone for codes over  $\mathbb{F}_3$  is discussed.

## I. INTRODUCTION

Low-density parity-check (LDPC) codes attract a lot of interest due to their excellent performance. For various communication channels, it was shown either analytically or empirically that LDPC-like codes attain capacity, when decoded by iterative message-passing algorithms (for example, see [5], [6], [7]).

In attempt to construct a framework for analysis of LDPC-like codes, it was observed by Wiberg that the message-passing algorithms operate locally on the Tanner graph of the code [9]. Therefore, the performance of the decoder is similar, whether it is applied to the Tanner graph itself, or to its so-called *graph cover*. This observation led to a definition of *computational tree pseudocodewords*. Later, a closely related concept of *graph-cover pseudocodewords* was extensively studied by Koetter and Vontobel [8]. These pseudocodewords were also found to be a reason for failure events of linear-programming decoder applied to binary linear codes [1], [2].

The graph-cover pseudocodewords, when viewed as points in the Euclidean space, lie inside a *fundamental cone* [4], [8]. The cone boundaries depend on the parity-check matrix of the code rather than on the code itself. For binary codes, the fundamental cone was thoroughly studied in [4]. However, as the size of the underlying field grows, the number of inequalities describing the boundaries of the fundamental cone also grows. In this work, we aim to extend the results in [4] towards codes defined over  $\mathbb{F}_3$  by providing a detailed characterization of the corresponding fundamental cone.

## II. DEFINITIONS AND SETTINGS

Let  $\mathcal{C}$  be a linear code of length  $n$  over a finite field  $\mathbb{F} \triangleq \mathbb{F}_q$  with  $q$  elements, and denote by  $\mathbb{F}^*$  a set of nonzero elements of  $\mathbb{F}$ . The code  $\mathcal{C}$  can be defined as

$$\mathcal{C} = \{c \in \mathbb{F}^n : cH^T = \mathbf{0}\} \quad (1)$$

where  $H$  is an  $m \times n$  matrix with entries from  $\mathbb{F}$  (called the *parity-check matrix* of  $\mathcal{C}$ ), and  $\mathbf{0}$  is all-zeros vector. Denote the set of column indices and the set of row indices of  $H$  by  $\mathcal{I} = \{1, 2, \dots, n\}$  and  $\mathcal{J} = \{1, 2, \dots, m\}$ , respectively. We use notation  $H_j$  for the  $j$ -th row of  $H$ , where  $j \in \mathcal{J}$ . Denote by  $\text{supp}(c)$  the support of a vector  $c$ . For each  $j \in \mathcal{J}$ , let  $\mathcal{I}_j = \text{supp}(H_j)$ . Denote by  $\|x\|$  a norm of a real vector  $x$ .

The Tanner graph of a linear code  $\mathcal{C}$  over  $\mathbb{F}$  is an equivalent characterization of the code's parity-check matrix  $H$ . The Tanner graph  $\mathcal{G} = (\mathcal{V}, \mathcal{E})$  has a vertex set  $\mathcal{V} = U \cup V$ , where  $U = \{u_i\}_{i \in \mathcal{I}}$  and  $V = \{v_j\}_{j \in \mathcal{J}}$ . There is an edge between  $u_i \in U$  and  $v_j \in V$  if and only if  $H_{j,i} \neq 0$ . This edge is labeled with the value  $H_{j,i}$ . We denote by  $\mathcal{N}(v)$  the set of neighbors of a vertex  $v \in \mathcal{V}$ .

To illustrate this concept, consider the following example from [3].

*Example 2.1:* Let  $\mathcal{C}$  be a  $[4, 2]$  linear code over  $\mathbb{F} = \mathbb{F}_3$  with parity-check matrix

$$H = \begin{pmatrix} 1 & 2 & 2 & 1 \\ 2 & 0 & 1 & 2 \end{pmatrix} \quad (2)$$

Figure 1 shows the Tanner graph for the codeword  $c = (1 \ 0 \ 2 \ 1)$  of the code  $\mathcal{C}$  with the parity-check matrix (2). Each vertex  $u_i \in U$  is labeled with the value of  $c_i$ . The reader may check that for each parity-check vertex  $v_j$ ,  $j = 1, 2$ , the sum, over all vertices in  $\mathcal{N}(v_j)$ , of the vertex labels multiplied by the corresponding edge labels is zero.

Next, we introduce the following two definitions from [4].

*Definition 2.1:* A graph  $\tilde{\mathcal{G}} = (\tilde{\mathcal{V}}, \tilde{\mathcal{E}})$  is a *finite cover* of the Tanner graph  $\mathcal{G} = (\mathcal{V}, \mathcal{E})$  if there exists a mapping  $\Pi : \tilde{\mathcal{V}} \rightarrow \mathcal{V}$  which is a graph homomorphism ( $\Pi$  takes adjacent vertices in  $\tilde{\mathcal{G}}$  to adjacent vertices in  $\mathcal{G}$ ), such that for every vertex  $v \in \mathcal{V}$  and every  $\tilde{v} \in \Pi^{-1}(v)$ , the neighborhood  $\mathcal{N}(\tilde{v})$  of  $\tilde{v}$  (including edge labels) is mapped bijectively to  $\mathcal{N}(v)$ .

*Definition 2.2:* A cover of the graph  $\mathcal{G}$  is said to have degree  $M$ , where  $M$  is a positive integer, if  $|\Pi^{-1}(v)| = M$  for every vertex  $v \in \mathcal{V}$ . We refer to such a cover graph as an *M-cover* of  $\mathcal{G}$ .

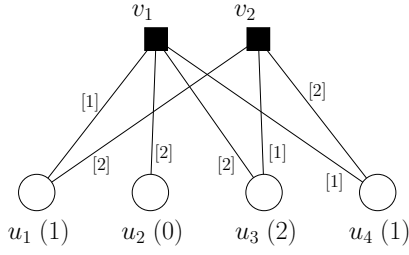


Fig. 1. Tanner graph for the example  $[4, 2]$  code  $\mathcal{C}$  over  $\mathbb{F}_3$  ([3]). Edge labels are shown in square brackets, and vertex labels in round brackets.

Fix some positive integer  $M$ . Let  $\tilde{\mathcal{G}} = (\tilde{\mathcal{V}}, \tilde{\mathcal{E}})$  be an  $M$ -cover of the Tanner graph  $\mathcal{G} = (\mathcal{V}, \mathcal{E})$  representing the code  $\mathcal{C}$  with a parity-check matrix  $\mathbf{H}$ . The vertices in the set  $\Pi^{-1}(u_i)$  are denoted  $\{u_{i,1}, u_{i,2}, \dots, u_{i,M}\}$ , where  $i \in \mathcal{I}$ . Similarly, the vertices in the set  $\Pi^{-1}(v_j)$  are denoted  $\{v_{j,1}, v_{j,2}, \dots, v_{j,M}\}$ , where  $j \in \mathcal{J}$ .

For any  $M \geq 1$ , a *graph-cover pseudocodeword* is a labeling of vertices  $u_{i,\mu}$  of the  $M$ -cover graph with values from  $\mathbb{F}$  such that all parity-checks are satisfied. We denote the label of  $u_{i,\mu}$  by  $\lambda(u_{i,\mu})$  and let  $p_{i,\mu} \triangleq \lambda(u_{i,\mu})$  for each  $i \in \mathcal{I}$ ,  $\mu = 1, 2, \dots, M$ . We may then write the graph-cover pseudocodeword in a vector form as

$$\mathbf{p} = (p_{1,1}, p_{1,2}, \dots, p_{1,M}, p_{2,1}, p_{2,2}, \dots, p_{2,M}, \dots, p_{n,1}, p_{n,2}, \dots, p_{n,M})$$

It is easily seen that  $\mathbf{p}$  belongs to a linear code  $\tilde{\mathcal{C}}$  of length  $Mn$  over  $\mathbb{F}$ , defined by an  $Mm \times Mn$  parity-check matrix  $\tilde{\mathbf{H}}$ . To construct  $\tilde{\mathbf{H}}$ , for  $1 \leq i^*, j^* \leq M$  and  $i \in \mathcal{I}$ ,  $j \in \mathcal{J}$ , we let  $i' = (i-1)M + i^*$ ,  $j' = (j-1)M + j^*$ , and so

$$\tilde{H}_{j',i'} = \begin{cases} H_{j,i} & \text{if } u_{i,i^*} \in \mathcal{N}(v_{j,j^*}) \\ 0 & \text{otherwise} \end{cases}$$

It may be seen that  $\tilde{\mathcal{G}}$  is the Tanner graph of the code  $\tilde{\mathcal{C}}$  corresponding to the parity-check matrix  $\tilde{\mathbf{H}}$ .

We also define the  $(q-1) \times n$  *unscaled graph-cover pseudocodeword matrix*

$$\mathbf{F} = \left( f_i^{(\alpha)} \right)_{\alpha \in \mathbb{F}^*; i \in \mathcal{I}}$$

where

$$f_i^{(\alpha)} = |\{\mu \in \{1, 2, \dots, M\} : p_{i,\mu} = \alpha\}| \geq 0$$

for  $i \in \mathcal{I}$ ,  $\alpha \in \mathbb{F}^*$ . For  $q = 2$ , graph-cover pseudocodeword matrix is actually a row vector of length  $n$ , and so in that case sometimes we use a vector notation rather than a matrix notation. The *normalized graph-cover pseudocodeword matrix* is defined as  $(1/M) \cdot \mathbf{F}$ .

It is straight-forward to see that for any  $\mathbf{c} \in \mathcal{C}$ , the labeling of  $u_{i,\mu}$  by the value  $c_i$  for all  $i \in \mathcal{I}$ ,  $\mu = 1, 2, \dots, M$ , trivially yields a pseudocodeword for all  $M$ -covers of  $\mathcal{G}$ ,  $M \geq 1$ . However, non-trivial pseudocodewords do exist.

*Example 2.2:* ([3]) Consider the ternary  $[4, 2]$  code  $\mathcal{C}$  in Example 2.1. Here we can take  $M = 4$ , so we have

$$\mathbf{p} = (1 \ 1 \ 2 \ 2 \mid 1 \ 1 \ 2 \ 2 \mid 0 \ 0 \ 1 \ 1 \mid 0 \ 0 \ 1 \ 1)$$

and the parity-check matrix of the code  $\tilde{\mathcal{C}}$  is given by

$$\tilde{\mathbf{H}} = \left( \begin{array}{cccc|cccc|cccc|cccc} 0 & 0 & 1 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & 0 & 0 \end{array} \right)$$

The unscaled graph-cover pseudocodeword matrix corresponding to  $\mathbf{p}$  is

$$\mathbf{F} = \left( \begin{array}{cccc} 2 & 2 & 2 & 2 \\ 2 & 2 & 0 & 0 \end{array} \right) \quad (3)$$

and the corresponding normalized graph-cover pseudocodeword matrix is  $\frac{1}{4} \cdot \mathbf{F}$ .

### III. BINARY CODES

Graph-cover pseudocodewords of *binary* codes were thoroughly studied in [4]. In particular, the characterization of a fundamental cone of the graph-cover pseudocodewords was given therein. In this section, we recall some results in [4].

In this section we consider a binary linear code  $\mathcal{C}$  (thus  $\mathbb{F} = \mathbb{F}_2$ ) with a parity-check matrix  $\mathbf{H}$ . The corresponding  $1 \times n$  graph-cover pseudocodeword matrix is thus a vector  $\mathbf{F} = (f_i^{(1)})_{i \in \mathcal{I}}$ . In this case, for the sake of simplicity, we will rather use notation  $\mathbf{F} = (f_i)_{i \in \mathcal{I}}$ .

*Definition 3.1:* A *binary fundamental cone* of  $\mathbf{H}$ , denoted  $\mathcal{K}_2(\mathbf{H})$ , is defined as the set of vectors  $\mathbf{x} \in \mathbb{R}^n$  that satisfy

$$\forall j \in \mathcal{J}, \forall \ell \in \mathcal{I}_j : f_\ell \leq \sum_{i \in \mathcal{I}_j \setminus \{\ell\}} f_i \quad (4)$$

$$\forall i \in \mathcal{I} : f_i \geq 0 \quad (5)$$

The following two theorems for characterization of the graph-cover pseudocodewords were presented in [4].

*Theorem 3.1:* Let  $\mathbf{F}$  be an  $1 \times n$  integer nonnegative matrix. Then the following two conditions are equivalent:

- 1)  $\mathbf{F}$  is an (unscaled) graph-cover pseudocodeword matrix.
- 2)  $\mathbf{F} \in \mathcal{K}_2(\mathbf{H})$  and  $\mathbf{H} \cdot \mathbf{F}^T = \mathbf{0} \pmod{2}$ .

*Theorem 3.2:* Let  $\mathcal{C}$  be a binary linear code with the parity-check matrix  $\mathbf{H}$ . Let  $\mathbf{z} \in \mathcal{K}_2(\mathbf{H})$  be a real vector of length  $n$ . Then, for any  $\epsilon > 0$ , there is an unscaled  $1 \times n$  pseudocodeword matrix (vector)  $\mathbf{F}$  such that  $\|c \cdot \mathbf{F} - \mathbf{z}\| < \epsilon$  for some real value  $c > 0$ .

### IV. TERNARY CODES

In this section, we study graph-cover pseudocodewords of codes over  $\mathbb{F} = \mathbb{F}_3$ . Assume that  $\mathcal{C}$  is a ternary linear code with a parity-check matrix  $\mathbf{H}$ .

*Definition 4.1:* A *ternary fundamental cone* of  $\mathbf{H}$ , denoted by  $\mathcal{K}_3(\mathbf{H})$ , is defined as the set of  $2 \times n$  matrices

$\mathbf{F} = (f_i^{(\alpha)})_{\alpha \in \mathbb{F}^*, i \in \mathcal{I}}$  with entries in  $\mathbb{R}$  that satisfy the following set of inequalities

$\forall j \in \mathcal{J}, \forall \ell \in \mathcal{I}_j :$

$$2 \sum_{i \in \mathcal{I}_j \setminus \{\ell\}} f_i^{(2H_{j,i})} + \sum_{i \in \mathcal{I}_j \setminus \{\ell\}} f_i^{(H_{j,i})} \geq 2f_\ell^{(H_{j,\ell})} + f_\ell^{(2H_{j,\ell})} \quad (6)$$

$$2 \sum_{i \in \mathcal{I}_j \setminus \{\ell\}} f_i^{(H_{j,i})} + \sum_{i \in \mathcal{I}_j \setminus \{\ell\}} f_i^{(2H_{j,i})} \geq 2f_\ell^{(2H_{j,\ell})} + f_\ell^{(H_{j,\ell})} \quad (7)$$

and,

$\forall j \in \mathcal{J}, \forall k, \ell \in \mathcal{I}_j :$

$$2 \sum_{i \in \mathcal{I}_j \setminus \{k, \ell\}} f_i^{(H_{j,i})} + \sum_{i \in \mathcal{I}_j} f_i^{(2H_{j,i})} \geq f_k^{(H_{j,k})} + f_\ell^{(H_{j,\ell})} \quad (8)$$

$$2 \sum_{i \in \mathcal{I}_j \setminus \{k, \ell\}} f_i^{(2H_{j,i})} + \sum_{i \in \mathcal{I}_j} f_i^{(H_{j,i})} \geq f_k^{(2H_{j,k})} + f_\ell^{(2H_{j,\ell})} \quad (9)$$

and, finally,

$$\forall i \in \mathcal{I}, \forall \alpha \in \mathbb{F}^* : f_i^{(\alpha)} \geq 0 \quad (10)$$

Here, all multiplications of type “ $2H_{j,i}$ ” are assumed to be over  $\mathbb{F}_3$ . If for some  $\mathbf{F}$  all inequalities (6)-(10) are satisfied (with respect to some  $\mathbf{H}$ ), we say that  $\mathbf{F} \in \mathcal{K}_3(\mathbf{H})$ .

*Example 4.1:* Consider the code in Example 2.1. The corresponding fundamental cone is given by the set of the following 32 inequalities.

From the second row of  $\mathbf{H}$ , inequalities (6) and (7) we have:

$$\begin{aligned} 2f_1^{(2)} + f_1^{(1)} &\leq 2(f_3^{(2)} + f_4^{(1)}) + (f_3^{(1)} + f_4^{(2)}) \\ 2f_1^{(1)} + f_1^{(2)} &\leq 2(f_3^{(1)} + f_4^{(2)}) + (f_3^{(2)} + f_4^{(1)}) \\ 2f_3^{(1)} + f_3^{(2)} &\leq 2(f_1^{(1)} + f_4^{(1)}) + (f_1^{(2)} + f_4^{(2)}) \\ 2f_3^{(2)} + f_3^{(1)} &\leq 2(f_1^{(2)} + f_4^{(2)}) + (f_1^{(1)} + f_4^{(1)}) \\ 2f_4^{(2)} + f_4^{(1)} &\leq 2(f_1^{(1)} + f_3^{(2)}) + (f_1^{(2)} + f_3^{(1)}) \\ 2f_4^{(1)} + f_4^{(2)} &\leq 2(f_1^{(2)} + f_3^{(1)}) + (f_1^{(1)} + f_3^{(2)}) \end{aligned}$$

From the second row of  $\mathbf{H}$ , inequalities (8) and (9):

$$\begin{aligned} f_1^{(2)} + f_3^{(1)} &\leq 2f_4^{(2)} + (f_1^{(1)} + f_3^{(2)} + f_4^{(1)}) \\ f_1^{(1)} + f_3^{(2)} &\leq 2f_4^{(1)} + (f_1^{(2)} + f_3^{(1)} + f_4^{(2)}) \\ f_1^{(2)} + f_4^{(2)} &\leq 2f_3^{(1)} + (f_1^{(1)} + f_3^{(2)} + f_4^{(1)}) \\ f_1^{(1)} + f_4^{(1)} &\leq 2f_3^{(2)} + (f_1^{(2)} + f_3^{(1)} + f_4^{(2)}) \\ f_3^{(1)} + f_4^{(2)} &\leq 2f_1^{(2)} + (f_1^{(1)} + f_3^{(2)} + f_4^{(1)}) \\ f_3^{(2)} + f_4^{(1)} &\leq 2f_1^{(1)} + (f_1^{(2)} + f_3^{(1)} + f_4^{(2)}) \end{aligned}$$

From the first row of  $\mathbf{H}$ , inequalities (6) and (7):

$$\begin{aligned} 2f_1^{(1)} + f_1^{(2)} &\leq 2(f_2^{(1)} + f_3^{(1)} + f_4^{(2)}) + (f_2^{(2)} + f_3^{(2)} + f_4^{(1)}) \\ 2f_1^{(2)} + f_1^{(1)} &\leq 2(f_2^{(2)} + f_3^{(2)} + f_4^{(1)}) + (f_2^{(1)} + f_3^{(1)} + f_4^{(2)}) \\ 2f_2^{(2)} + f_2^{(1)} &\leq 2(f_1^{(2)} + f_3^{(1)} + f_4^{(2)}) + (f_1^{(1)} + f_3^{(2)} + f_4^{(1)}) \\ 2f_2^{(1)} + f_2^{(2)} &\leq 2(f_1^{(1)} + f_3^{(2)} + f_4^{(1)}) + (f_1^{(2)} + f_3^{(1)} + f_4^{(2)}) \\ 2f_3^{(2)} + f_3^{(1)} &\leq 2(f_1^{(2)} + f_2^{(1)} + f_4^{(2)}) + (f_1^{(1)} + f_2^{(2)} + f_4^{(1)}) \\ 2f_3^{(1)} + f_3^{(2)} &\leq 2(f_1^{(1)} + f_2^{(2)} + f_4^{(1)}) + (f_1^{(2)} + f_2^{(1)} + f_4^{(2)}) \end{aligned}$$

$$\begin{aligned} 2f_4^{(1)} + f_4^{(2)} &\leq 2(f_1^{(2)} + f_2^{(1)} + f_3^{(1)}) + (f_1^{(1)} + f_2^{(2)} + f_3^{(2)}) \\ 2f_4^{(2)} + f_4^{(1)} &\leq 2(f_1^{(1)} + f_2^{(2)} + f_3^{(2)}) + (f_1^{(2)} + f_2^{(1)} + f_3^{(1)}) \end{aligned}$$

Finally, from the first row of  $\mathbf{H}$ , inequalities (8) and (9), we obtain additional 12 inequalities, which we will omit here.

Take, for example, a graph-cover pseudocodeword matrix in (3). It can be easily checked that this pseudocodeword matrix satisfies all 32 inequalities above.

Let  $\mathcal{C}$  be a linear code of length  $n$  over  $\mathbb{F}$ , and let  $\mathbf{H}$  be its parity-check matrix. Suppose  $\mathcal{C}_j$  (for all  $j \in \mathcal{J}$ ) is a code, whose parity-check matrix is given by  $\mathbf{H}_j$ .

*Lemma 4.1:* The following connection holds:

$$\mathcal{K}_3(\mathbf{H}) = \mathcal{K}_3(\mathbf{H}_1) \cap \mathcal{K}_3(\mathbf{H}_2) \cap \cdots \cap \mathcal{K}_3(\mathbf{H}_m)$$

*Lemma 4.2:* Let  $\mathbf{F} = (f_i^{(\alpha)})_{\alpha \in \mathbb{F}^*, i \in \mathcal{I}}$  be an unscaled graph-cover pseudocodeword matrix of  $\mathcal{C}_j$  (with respect to  $\mathbf{H}_j$ ) for all  $j \in \mathcal{J}$ . Then,  $\mathbf{F}$  is a graph-cover pseudocodeword matrix of  $\mathcal{C}$  (with respect to  $\mathbf{H}$ ).

For  $j \in \mathcal{J}$ , define the mapping  $\psi_{\mathbf{H}_j} : \mathbb{R}^{2 \times n} \rightarrow \mathbb{R}^{2 \times n}$  as follows. For all  $\mathbf{F} \in \mathbb{R}^{2 \times n}$ , all  $\alpha \in \mathbb{F}^*$  and  $i \in \mathcal{I}$ , the entry in row  $\alpha$  and column  $i$  of  $\hat{\mathbf{F}} \triangleq \psi_{\mathbf{H}_j}(\mathbf{F})$  is

$$\hat{f}_i^{(\alpha)} = \begin{cases} f_i^{(-\alpha)} & \text{if } H_{j,i} = 2 \\ f_i^{(\alpha)} & \text{otherwise} \end{cases}$$

where the upper indices  $-\alpha$  and  $\alpha$  are taken over  $\mathbb{F}$ . In other words, we exchange entries  $f_i^{(1)}$  and  $f_i^{(2)}$  whenever  $H_{j,i} = 2$ .

Let  $\mathbf{H}_s$  be a  $1 \times n$  matrix obtained by replacing every nonzero entry in  $\mathbf{H}_j$  by a unity in  $\mathbb{F}$ . Then, we have the following lemma.

*Lemma 4.3:* Let  $\mathcal{C}_j$ ,  $\mathbf{H}_j$  and  $\mathbf{H}_s$  be as defined above. Let  $\mathbf{F} \in \mathbb{R}^{2 \times n}$ . Then,

- 1)  $\mathbf{F} \in \mathcal{K}_3(\mathbf{H}_j)$  if and only if  $\psi_{\mathbf{H}_j}(\mathbf{F}) \in \mathcal{K}_3(\mathbf{H}_s)$ ;
- 2)  $\mathbf{F}$  is a graph-cover pseudocodeword matrix of the code  $\mathcal{C}_j$  with respect to the parity-check matrix  $\mathbf{H}_j$  if and only if  $\psi_{\mathbf{H}_j}(\mathbf{F})$  is a graph-cover pseudocodeword matrix of the code defined by the parity-check matrix  $\mathbf{H}_s$ .

*Example 4.2:* Consider the matrix  $\mathbf{H}$  in Example 2.1. Let  $\mathcal{C}_2$  be the code over  $\mathbb{F}$  checked by  $\mathbf{H}_2$  (the second row of  $\mathbf{H}$ ). Then,

$$\mathbf{F} = \begin{pmatrix} 2 & 2 & 2 & 2 \\ 2 & 2 & 0 & 0 \end{pmatrix}$$

is a graph-cover pseudocodeword matrix of  $\mathcal{C}_2$  with respect to  $\mathbf{H}_2$ , and

$$\hat{\mathbf{F}} = \psi_{\mathbf{H}_2}(\mathbf{F}) = \begin{pmatrix} 2 & 2 & 2 & 0 \\ 2 & 2 & 0 & 2 \end{pmatrix}$$

is a graph-cover pseudocodeword matrix of the code checked by the  $1 \times 4$  matrix  $\mathbf{H}_s = [1 \ 0 \ 1 \ 1]$ .

The last three lemmas allows us to simplify the task of characterization of the graph-cover pseudocodewords. Lemmas 4.1 and 4.2 indicate that we can consider  $m$  codes  $\mathcal{C}_j$ ,  $j \in \mathcal{J}$ , each code is checked by a single parity-check row  $\mathbf{H}_j$  of  $\mathbf{H}$ . The

characterization of the pseudocodewords corresponding to  $\mathbf{H}$  is derived from the characterizations of pseudocodewords of each of  $\mathbf{H}_j$ 's. Lemma 4.3 suggests, in turn, that in order to characterize the graph-cover pseudocodewords of a code, it is enough to consider only matrices  $\mathbf{H}_s$  with entries equal zero and one only (but not two).

The next lemma refers to  $\mathbf{F}$  containing an all-zero row.

**Lemma 4.4:** Let  $\mathbf{F} = (f_i^{(\alpha)})_{\alpha \in \mathbb{F}^*, i \in \mathcal{I}}$  be a  $2 \times n$  integer matrix with nonnegative entries. Assume that  $\mathbf{H}_s$  is  $1 \times n$  matrix with entries in  $\{0, 1\} \subset \mathbb{F}$ , and  $\mathbf{F} \in \mathcal{K}_3(\mathbf{H}_s)$ . W.l.o.g. suppose that  $f_i^{(2)} = 0$  for all  $i \in \mathcal{I}$  and  $\sum_{i \in \mathcal{I}} f_i^{(1)} = 0 \pmod 3$  (for case where  $f_i^{(1)} = 0$  for all  $i \in \mathcal{I}$ , switch between  $f_i^{(1)}$  and  $f_i^{(2)}$  for all  $i$ ). Then there exist sets of indices  $S_1, S_2, \dots, S_M \subseteq \mathcal{I}$ , such that for every set  $S_\mu$ ,  $\mu = 1, 2, \dots, M$ , it holds

$$|S_\mu| = 0 \pmod 3$$

and for every index  $i \in \mathcal{I}$ , the number of sets  $S_\mu$  in which  $i$  appears equals to  $f_i^{(1)}$ .

The next lemma is a generalization of Lemma 4.4 for the case when both  $f_i^{(1)}$  and  $f_i^{(2)}$  are possibly nonzero (for some  $i$ 's).

**Lemma 4.5:** Suppose that  $\mathbf{F} = (f_i^{(\alpha)})_{\alpha \in \mathbb{F}^*, i \in \mathcal{I}}$  is a  $2 \times n$  integer matrix with nonnegative entries. Assume that  $\mathbf{H}_s$  is  $1 \times n$  matrix with entries in  $\{0, 1\} \subset \mathbb{F}$ , and it serves as a parity-check matrix of the ternary linear code  $\mathcal{C}_s$ . Let  $\mathbf{F} \in \mathcal{K}_3(\mathbf{H}_s)$ , and

$$\mathbf{H}_s \cdot (\mathbf{F}_1^T + 2\mathbf{F}_2^T) = 0 \pmod 3 \quad (11)$$

when  $\mathbf{H}_s$  is regarded as an integer matrix, and  $\mathbf{F}_1$  and  $\mathbf{F}_2$  are the first and the second rows of  $\mathbf{F}$ , respectively. Then  $\mathbf{F}$  is an (unscaled) graph-cover pseudocodeword matrix of  $\mathcal{C}_s$  corresponding to (some graph cover of)  $\mathbf{H}_s$ .

Before we discuss the proof of Lemma 4.5, we first introduce a new definition.

**Definition 4.2:** Let  $(f_i^{(\alpha)})_{\alpha \in \mathbb{F}^*, i \in \mathcal{I}}$  be a graph-cover pseudocodeword matrix corresponding to a code  $\mathcal{C}_j$  checked by the  $1 \times n$  parity-check matrix  $\mathbf{H}_j$  over  $\mathbb{F}$ , and let  $\mathcal{I}_j = \text{supp}(\mathbf{H}_j)$ .

- If for some  $\ell \in \mathcal{I}_j$ ,  $\sum_{\alpha \in \mathbb{F}^*} f_\ell^{(\alpha)} \geq 1$  and

$$2 \sum_{i \in \mathcal{I}_j \setminus \{\ell\}} f_i^{(2H_{1,i})} + \sum_{i \in \mathcal{I}_j \setminus \{\ell\}} f_i^{(H_{1,i})} < 2f_\ell^{(H_{1,\ell})} + f_\ell^{(2H_{1,\ell})} + 3$$

then this equation is *critical* and the coordinate  $\ell$  is *critical of type one*.

- Similarly, if for some  $\ell \in \mathcal{I}_j$ ,  $\sum_{\alpha \in \mathbb{F}^*} f_\ell^{(\alpha)} \geq 1$  and

$$2 \sum_{i \in \mathcal{I}_j \setminus \{\ell\}} f_i^{(H_{1,i})} + \sum_{i \in \mathcal{I}_j \setminus \{\ell\}} f_i^{(2H_{1,i})} < 2f_\ell^{(2H_{1,\ell})} + f_\ell^{(H_{1,\ell})} + 3$$

then this equation is *critical* and the coordinate  $\ell$  is *critical of type two*.

- If for some  $k, \ell \in \mathcal{I}_j$ ,  $f_k^{(H_{1,k})} \geq 1$  and  $f_\ell^{(H_{1,\ell})} \geq 1$  and

$$2 \sum_{i \in \mathcal{I}_j \setminus \{k, \ell\}} f_i^{(H_{1,i})} + \sum_{i \in \mathcal{I}_j} f_i^{(2H_{1,i})} < f_k^{(H_{1,k})} + f_\ell^{(H_{1,\ell})} + 3$$

then this equation is *critical* and the pair of coordinates  $\{k, \ell\}$  is *critical of type one*.

- If for some  $k, \ell \in \mathcal{I}_j$ ,  $f_k^{(2H_{1,k})} \geq 1$  and  $f_\ell^{(2H_{1,\ell})} \geq 1$  and

$$2 \sum_{i \in \mathcal{I}_j \setminus \{k, \ell\}} f_i^{(2H_{1,i})} + \sum_{i \in \mathcal{I}_j} f_i^{(H_{1,i})} < f_k^{(2H_{1,k})} + f_\ell^{(2H_{1,\ell})} + 3$$

then this equation is *critical* and the pair of coordinates  $\{k, \ell\}$  is *critical of type two*.

**Lemma 4.6:** Let  $\mathbf{H}_j$  be  $1 \times n$  parity-check matrix of a linear code over  $\mathbb{F}$ , and let  $\mathbf{F} \in \mathcal{K}_3(\mathbf{H}_j)$  be a  $2 \times n$  nonnegative integer matrix, such that (11) holds (with respect to  $\mathbf{H}_j$ ). Assume that some of inequalities (6)-(9) are critical. Then, all the critical inequalities can be rewritten as equalities without “+3” term in the right-hand side.

*Sketch of the Proof of Lemma 4.5.*

Denote  $\mathcal{I}_s \triangleq \text{supp}(\mathbf{H}_s)$ . Let  $\mathbf{F} \in \mathcal{K}_3(\mathbf{H}_s)$  be a  $2 \times n$  integer nonnegative matrix satisfying (11). We construct a graph cover  $\tilde{\mathcal{G}} = (\mathcal{V}, \tilde{\mathcal{E}})$ , corresponding to this  $\mathbf{F}$ .

For initialization, we take

$$M' \triangleq \max_{i \in \mathcal{I}} \left\{ \sum_{\alpha \in \mathbb{F}^*} f_i^{(\alpha)} \right\}, \quad M \triangleq 3M' - 2$$

and

$$U = \{u_{1,1}, u_{1,2}, \dots, u_{1,M}, u_{2,1}, u_{2,2}, \dots, u_{2,M}, \\ u_{n,1}, u_{n,2}, \dots, u_{n,M}\}$$

$$V = \{v_1, v_2, \dots, v_M\}, \quad \tilde{\mathcal{V}} = U \cup V, \quad \tilde{\mathcal{E}} = \emptyset$$

For all  $u_{i,\mu} \in U$ ,  $i \in \mathcal{I}_s$ , we set labels  $\lambda(u_{i,\mu}) = 0$ . For  $i \in \mathcal{I} \setminus \mathcal{I}_s$  we set labels  $\lambda(u_{i,\mu}) = \alpha$  ( $\alpha \in \mathbb{F}^*$ ) for  $f_i^{(\alpha)}$  arbitrary vertices  $u_{i,\mu} \in U$ . For the remaining vertices  $u_{i,\mu} \in U$  (with  $i \in \mathcal{I} \setminus \mathcal{I}_s$ ) we set  $\lambda(u_{i,\mu}) = 0$ .

The algorithm for construction of the graph cover works in steps. On each step, we reduce two (or three) entries in  $\mathbf{F}$  by one, and at the same time add two (or three) corresponding edges to  $\tilde{\mathcal{E}}$ . We do it in a way such that the new  $\mathbf{F}$  is in  $\mathcal{K}_3(\mathbf{H}_s)$  and also satisfies (11).

The definition of critical coordinates implies that if there is a critical coordinate  $\ell$  (of either type one or two), then either entry  $f_\ell^{(1)}$  or  $f_\ell^{(2)}$  has to be reduced (otherwise, some of critical inequalities in (6)-(9) might be violated after the reduction). Moreover, if there is a critical pair of coordinates  $\{k, \ell\}$  of type  $\alpha$  ( $\alpha \in \mathbb{F}^*$ ), then either  $f_k^{(\alpha)}$  or  $f_\ell^{(\alpha)}$  has to be reduced (due to the same reason). Any non-critical inequalities remain valid after any such reduction.

The formal description of the algorithm for reduction of  $\mathbf{F}$  appears in Figure 2. We use notation  $S_c \subseteq \mathcal{I}$  for a set of all critical coordinates,  $T_1$  for a set of critical pairs of coordinates of type one, and  $T_2$  for a set of critical pairs of coordinates of type two. These sets are assumed to be updated in the beginning of each iteration in Stage 2 of the algorithm.

The main challenge in the proof of the algorithm correctness is to show that for any  $\mathbf{F} \in \mathcal{K}_3(\mathbf{H}_s)$  satisfying (11), and for any possible combination of critical coordinates, the reduction

---

**Input:**  $H_s, F = (f_i^{(\alpha)})_{\alpha \in \mathbb{F}^*, i \in \mathcal{I}}$ .

1. **Initialize:**  $M, U, V, \tilde{\mathcal{G}} = (\tilde{V}, \tilde{\mathcal{E}})$ , and  $\lambda(u_{i,\mu})$  for all  $u_{i,\mu} \in U$ .
2. **While**  $\sum_{i \in \mathcal{I}_s} f_i^{(\alpha)} \neq 0$  **for all**  $\alpha \in \mathbb{F}^*$  **do:**  
Find  $k$  and  $\ell$  such that:
  - 1)  $f_k^{(1)} \geq 1$  and  $f_\ell^{(2)} \geq 1$ ;
  - 2) for all  $i \in S_c$ : either  $i = k$  or  $i = \ell$ ;
  - 3) for all  $\{i_1, i_2\} \in T_1$ : either  $i_1 = k$  or  $i_2 = \ell$ ;
  - 4) for all  $\{i_1, i_2\} \in T_2$ : either  $i_1 = \ell$  or  $i_2 = k$ . $\mu_k \leftarrow \sum_{\alpha \in \mathbb{F}^*} f_k^{(\alpha)}, \quad \mu_\ell \leftarrow \sum_{\alpha \in \mathbb{F}^*} f_\ell^{(\alpha)}$ .  
 $f_k^{(1)} \leftarrow f_k^{(1)} - 1, f_\ell^{(2)} \leftarrow f_\ell^{(2)} - 1, \lambda(v_{k,\mu_k}) \leftarrow 1, \lambda(v_{\ell,\mu_\ell}) \leftarrow 2$   
Take  $v_\mu$  not connected to  $u_{k,\eta}, u_{\ell,\eta}$  for any  $\eta = 1, \dots, M$ .  
 $\tilde{\mathcal{E}} \leftarrow \tilde{\mathcal{E}} \cup \{\{u_{k,\mu_k}, v_\mu\}, \{u_{\ell,\mu_\ell}, v_\mu\}\}$ .
3. **While**  $f_i^{(\alpha)} \neq 0$  **for some**  $i \in \mathcal{I}_s, \alpha \in \mathbb{F}^*$  **do:**  
Let  $f_{\ell_1}^{(\beta)}, f_{\ell_2}^{(\beta)}, f_{\ell_3}^{(\beta)}$  be three largest entries in  $F$ .  
 $\mu_1 \leftarrow f_{\ell_1}^{(\beta)}, \mu_2 \leftarrow f_{\ell_2}^{(\beta)}, \mu_3 \leftarrow f_{\ell_3}^{(\beta)}$ .  
For  $i = 1, 2, 3$ :  $f_{\ell_i}^{(\beta)} \leftarrow f_{\ell_i}^{(\beta)} - 1, \lambda(u_{i,\mu_i}) \leftarrow \beta$ .  
Take  $v_\mu$  not connected to  $u_{\ell_i,\eta}$ , for  $i = 1, 2, 3, \eta = 1, \dots, M$ .  
 $\tilde{\mathcal{E}} \leftarrow \tilde{\mathcal{E}} \cup \{\{u_{\ell_1,\mu_1}, v_\mu\}, \{u_{\ell_2,\mu_2}, v_\mu\}, \{u_{\ell_3,\mu_3}, v_\mu\}\}$ .
4. **For all**  $i \in \mathcal{I}_s$  **and**  $\mu_1 = 1, \dots, M$  **such that**  $\lambda(u_{i,\mu_1}) = 0$ :  
  - 1) Pick  $\mu$  s.t.  $\{u_{i,\eta}, v_\mu\} \notin \tilde{\mathcal{E}}$  for any  $\eta = 1, 2, \dots, M$ ;
  - 2)  $\tilde{\mathcal{E}} \leftarrow \tilde{\mathcal{E}} \cup \{\{u_{i,\mu_1}, v_\mu\}\}$ .

**Output:**  $\tilde{\mathcal{G}}$ .

---

Fig. 2. Algorithm for constructing the graph cover  $\tilde{\mathcal{G}}$ .

of the entries of  $F$  as above is always possible. We omit further details due to the lack of space.

*Example 4.3:* To illustrate the algorithm, consider the parity-check matrix  $H_s$  in Example 4.2 and the corresponding pseudocodeword matrix  $\hat{F}$ . Then  $M' = 4$  (and so  $M = 10$ , although  $M = 4$  would be sufficient). It can be easily seen that the coordinate  $\ell = 1$  is critical of both types one and two. In addition, the pairs of coordinates  $\{k_1, \ell_1\} = \{1, 3\}$  and  $\{k_2, \ell_2\} = \{1, 4\}$  are critical of type one and two, respectively. Therefore, the algorithm has to reduce  $f_1^{(\alpha)}$  for some  $\alpha \in \mathbb{F}^*$ . Suppose that  $f_1^{(2)}$  ( $\ell = 1, \alpha = 2$ ) was selected for reduction. This implies, in turn, that  $k = 3$ . Thus, the algorithm sets  $\lambda(u_{1,4}) = 2$  and  $\lambda(u_{3,2}) = 1$ . The edges  $\{u_{1,4}, v_1\}$  and  $\{u_{3,2}, v_1\}$  are added to  $\tilde{\mathcal{E}}$ . The new  $\hat{F}$  is:

$$\hat{F} = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 2 \end{pmatrix}$$

For this  $\hat{F}$ , the same critical conditions hold as before, and so  $f_1^{(\alpha)}$  (for some  $\alpha \in \mathbb{F}^*$ ) is reduced again. Suppose that the same  $\alpha, k$  and  $\ell$  were selected again, and so  $\lambda(u_{1,3}) = 2$  and  $\lambda(u_{3,1}) = 1$ , and the edges  $\{u_{1,3}, v_2\}$  and  $\{u_{3,1}, v_2\}$  are added to  $\tilde{\mathcal{E}}$ . We obtain

$$\hat{F} = \begin{pmatrix} 2 & 2 & 0 & 0 \\ 0 & 2 & 0 & 2 \end{pmatrix}$$

At this point, the coordinates  $k = 1$  and  $\ell = 4$  are both critical. Therefore, we set  $\lambda(u_{1,2}) = 1$  and  $\lambda(u_{4,2}) = 2$ , and the edges  $\{u_{1,2}, v_3\}$  and  $\{u_{4,2}, v_3\}$  are added to  $\tilde{\mathcal{E}}$ . The entries  $f_1^{(1)}$  and  $f_4^{(2)}$  are reduced.

Then, again,  $\lambda(u_{1,1}) = 1$  and  $\lambda(u_{4,1}) = 2$ , and the edges  $\{u_{1,1}, v_4\}$  and  $\{u_{4,1}, v_4\}$  are added to  $\tilde{\mathcal{E}}$ , and the entries  $f_1^{(1)}$

and  $f_4^{(2)}$  are reduced. To this end  $f_i^{(\alpha)} = 0$  for all  $\alpha \in \mathbb{F}^*$  and  $i \in \mathcal{I}_s$ . Additional 22 edges connecting zero-labeled vertices with the parity-check vertices are added to  $\tilde{\mathcal{E}}$ . The algorithm outputs the resulting  $\tilde{\mathcal{G}}$  and stops.

The following two theorems are the main result of this paper.

*Theorem 4.7:* Let  $\mathcal{C}$  be a linear ternary code of length  $n$  over  $\mathbb{F}$ , and  $H$  is its parity-check matrix. Let  $F$  be a  $2 \times n$  matrix with non-negative integer entries. Then, the following two conditions are equivalent.

- 1)  $F$  is an (unscaled) graph-cover pseudocodeword matrix of  $\mathcal{C}$  corresponding to (the graph cover of)  $H$ .
- 2)  $F \in \mathcal{K}_3(H)$  and

$$H \cdot (F_1^T + 2F_2^T) = 0 \pmod{3}$$

where  $H$  is regarded as an integer matrix.

*Theorem 4.8:* Let  $\mathcal{C}$  be a ternary linear code with the parity-check matrix  $H$ . Let  $Z \in \mathcal{K}_3(H)$  be a  $2 \times n$  real matrix. Then, for any  $\epsilon > 0$ , there is an unscaled graph-cover pseudocodeword matrix  $F$  such that  $\|c \cdot F - Z\| < \epsilon$  for some real value  $c > 0$ .

## ACKNOWLEDGMENTS

The author would like to thank Eimear Byrne, Mark F. Flanagan and Marcus Greferath for many inspiring discussions. The author also wishes to thank Yeow Meng Chee.

This work was done in part while the author was with the Claude Shannon Institute, University College Dublin. This work was supported in part by the Science Foundation Ireland (Claude Shannon Institute for Discrete Mathematics, Coding and Cryptography, Grant 06/MI/006), and in part by the National Research Foundation of Singapore (Research Grant NRF-CRP2-2007-03).

## REFERENCES

- [1] J. Feldman, *Decoding Error-Correcting Codes via Linear Programming*. Ph.D. Thesis, Massachusetts Institute of Technology, Sep. 2003.
- [2] J. Feldman, M. J. Wainwright, and D. R. Karger, "Using linear programming to decode binary linear codes," *IEEE Transactions on Information Theory*, vol. 51, no. 3, pp. 954–972, March 2005.
- [3] M.F. Flanagan, V. Skachek, E. Byrne, and M. Greferath, "Linear-programming decoding of non-binary linear codes," *IEEE Transactions on Information Theory*, vol. 55, no. 9, pp. 4134–4154, September 2009.
- [4] 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.
- [5] M. Luby, M. Mitzenmacher, A. Shokrollahi, and D. Spielman, "Efficient erasure correcting codes," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 569–584, Feb. 2001.
- [6] P. Oswald and A. Shokrollahi, "Capacity-achieving sequences for the erasure channel," *IEEE Transactions on Information Theory*, vol. 48, no. 12, pp. 3017–3028, Dec. 2002.
- [7] T. Richardson, A. Shokrollahi, and R. Urbanke, "Design of capacity-approaching low-density parity-check codes," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 619–637, Feb. 2001.
- [8] P. Vontobel and R. Koetter, "Graph-cover decoding and finite-length analysis of message-passing iterative decoding of LDPC codes," to appear in *IEEE Transactions on Information Theory*, Arxiv report arXiv:cs.IT/0512078, Dec. 2005.
- [9] N. Wiberg, *Codes and Decoding on General Graphs*. Ph.D. Thesis, Linköping University, Sweden, 1996.