This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TIT.2014.2331677

Pseudocodewords of Parity-Check Codes over Fields of Prime Cardinality

Wittawat Kositwattanarerk and Gretchen L. Matthews, *Senior Member, IEEE*

***Abstract*—This paper considers pseudocodewords of LDPC codes over alphabets with prime cardinality p for use over the p-ary symmetric channel. Pseudocodewords are decoding algorithm outputs that may not be legitimate codewords. Here, we consider pseudocodewords arising from graph cover decoding and linear programming decoding. For codes over the binary alphabet, such pseudocodewords correspond to rational points of the fundamental polytope. They can be characterized via the fundamental cone which is the conic hull of the fundamental polytope; the pseudocodewords are precisely those integer vectors within the fundamental cone that reduce modulo 2 to a codeword. In this paper, we determine a set of conditions that pseudocodewords of codes over $\mathbb{F}_p$, the finite field of prime cardinality p, must satisfy. To do so, we introduce a class of critical multisets and a mapping which associates a real number to each pseudocodeword over $\mathbb{F}_p$. The real numbers associated with pseudocodewords are subject to lower bounds imposed by the critical multisets. The inequalities are given in terms of the parity-check matrix entries and critical multisets. This gives a necessary and sufficient condition for pseudocodewords of codes over $\mathbb{F}_2$ and $\mathbb{F}_3$ and a necessary condition for those over larger alphabets. In addition, irreducible pseudocodewords of codes over $\mathbb{F}_3$ are found as a Hilbert basis for the lifted fundamental cone.**

***Index Terms*—iterative decoding, low-density parity-check (LDPC) code, fundamental cone, pseudocodewords, irreducible pseudocodewords, nonbinary code**

I. Introduction

LOW-density parity-check (LDPC) codes have received much attention due to the fact that certain families of such codes have been shown to approach capacity over large classes of channels when paired with iterative message-passing decoding algorithms. One drawback of these decoding algorithms is that they may produce noncodeword outputs, called pseudocodewords. Because there are various types of decoding algorithms for parity-check codes (especially for LDPC codes), several kinds of pseudocodewords exist in the literature. In this introduction, we use the term pseudocodeword rather generically to facilitate the discussion while avoiding technicalities. In the next section, we will make precise the definitions of the types of pseudocodewords we consider and keep that level of rigor throughout the remainder of the paper.

Pseudocodewords of binary codes have been studied extensively in the literature. In particular, analysis of pseudocodewords as a means to understand iterative message-passing decoding algorithms began in the work of Wiberg [27] where computation trees were used to backtrack the calculations done by the algorithms. In [18], [26], Koetter and Vontobel analyzed the pseudocodewords using a finite degree lift of the Tanner graph called a graph cover. They also introduced the fundamental polytope whose rational points correspond to pseudocodewords. Taking the conic hull of the fundamental polytope yields the fundamental cone, a convex cone that contains all pseudocodewords of a binary code; its description can be simpler than that of the fundamental polytope while encapsulating the information relevant to pseudocodewords. Generators of this cone are called minimal pseudocodewords.

Bounds on the weights of minimal pseudocodewords were given in [15] (see also [26]) along with a definition of irreducible pseudocodewords, which are building blocks for pseudocodewords. The pseudocodewords within the fundamental cone were characterized by Koetter et al. [17]. It turns out that these pseudocodewords coincide with noncodeword outputs of linear programming decoding [6], [7], and connections among different types of pseudocodewords were discussed in [1]. Nonetheless, most discussions on the pseudocodewords thus far focused on codes over the binary alphabet.

The application of nonbinary LDPC codes was first considered in 1998 by Davey and MacKay [5]. Their

W. Kositwattanarerk is with the Department of Mathematics, Faculty of Science, Mahidol University, Bangkok 10400, Thailand and is with the Centre of Excellence in Mathematics, the Commission on Higher Education, Bangkok 10400, Thailand. (e-mail: wittawat.kos@mahidol.edu).

G. L. Matthews is with the Department of Mathematical Sciences, Clemson University, Clemson, SC 29634-0975, USA (e-mail: gmatthe@clemson.edu). The work of this author is supported by NSF DMS-0901693 and NSA H-98230-06-1-0008.

Copyright (c) 2014 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org

Copyright (c) 2014 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TIT.2014.2331677

Monte Carlo simulations demonstrated that codes over finite fields of size greater than 2 have significantly improved performance over binary codes. This calls for an investigation of nonbinary LDPC codes. Pseudocodewords of nonbinary codes were defined by Kelley et al. [16] in 2006 and revisited with the introduction of linear programming decoding for nonbinary codes [8], [24]. The fundamental cone was then generalized to codes over the ternary alphabet in [22]. While it has been noted that codes over larger alphabets are more appropriate for certain applications, thorough analysis of nonbinary LDPC codes remains. As a step in this direction, we consider p-ary LDPC codes where p is a prime. The results presented here may be applied to any p-ary parity-check code, though it is more natural to do so when the code is represented by a low-density parity-check matrix. One may consider this as an initial step in the study of LDPC codes over arbitrary finite fields.

Recent work on nonbinary LDPC codes includes that of Burshtein and Goldenberg [2] and Goldin and Burshtein [12]. In [2], the authors provide a procedure for obtaining the fundamental polytope of a parity-check code. Their approach relies on the double description method which is an algorithm for extreme ray enumeration. While the double description method can be quite practical for certain problems when implemented with particular heuristic strategies, it can be exponential in the input size and its running time depends substantially on choices made in the execution of the algorithm. See [11] for a thorough discussion of the double description method. In [2], it is applied to LDPC codes over finite rings to give facet representations of the local code polytopes (from their vertex descriptions). This procedure can be implemented computationally to yield facet defining inequalities and is said to work reasonably well only if the code is small.

In this paper, we explore pseudocodewords of nonbinary parity-check codes over the p-ary symmetric channel, where p is the size of the input alphabet. Our approach is via the fundamental cone, and we seek the inequalities that define this cone. Our work differs from that of Burshtein and Goldenberg in that it relies on a combinatorial notion, termed a critical multiset, that we introduce in this paper. It yields inequalities that the pseudocodewords of a p-ary code must satisfy. An advantage of our method is that the inqualities come directly from the parity-check matrix and the set of partitions of $p-1$. A drawback is that the cone defined by these inequalities may be strictly larger than the fundamental cone for larger values of p. While our method applies only to codes over fields of prime cardinality (as opposed to more general finite rings), it does not rely on an underlying algorithm which is sensitive to issues such as the ordering of rows of the parity-check matrix and whose efficient implementation is a current topic of research.

This paper is organized as follows. A summary of notation is provided at the end of this section and relevant background is covered in Section II. Section III discusses p-ary pseudocodewords. Here, we determine inequalities that define a cone containing all p-ary pseudocodewords. For $p = 2$ (resp. $p = 3$), this cone coincides with the fundamental cone as defined by Koetter and Vontobel [18] (resp. Skachek [22]). The ternary case is considered in greater detail in Section IV where pseudocodewords are found as integer points in a lifting of the cone defined in the previous section. The final sections, Sections V and VI, contain examples and the conclusion.

Notation. The set of real numbers is denoted $\mathbb{R}$, $\mathbb{Z}$ is the set of integers, and $\mathbb{Q}$ is the set of rational numbers. The set of nonnegative integers is denoted by $\mathbb{N}$, the set of nonnegative real numbers is denoted by $\mathbb{R}_{\geq 0}$, and the set of positive real numbers is written $\mathbb{R}_{+}$. The set of all $r \times n$ matrices with entries in a field $\mathbb{F}$ is denoted $\mathbb{F}^{r\times n}$, and $\mathbb{F}^n \coloneqq \mathbb{F}^{1\times n}$. Given a matrix $H \in \mathbb{F}^{r\times n}$, h_{ji} denotes the entry of H in the j^{th} row and i^{th} column, $\mathrm{Row}_j(H)$ denotes the j^{th} row of H, $\mathrm{Col}_i(H)$ denotes the i^{th} column of H, and H^T denotes the transpose of H. The support of $\mathrm{Row}_j(H)$ is $\mathrm{supp}\left(\mathrm{Row}_j(H)\right) \coloneqq \{i : h_{ji} \neq 0\}$. The i^{th} coordinate of a vector $\mathbf{v} \in \mathbb{R}^n$ is denoted v_i. Given a prime p, the finite field with p elements is denoted $\mathbb{F}_p \coloneqq \{0, 1, \ldots, p-1\}$, and $\mathbb{F}_p^* \coloneqq \mathbb{F}_p \setminus \{0\}$. Finite field multiplication is denoted by $\odot$ if it is not clear from the context.

We adopt the conventional coding theory terminology and notation. A linear code C over a finite field $\mathbb{F}$ of length n and dimension k is a subspace of $\mathbb{F}^n$ of dimension k; we use the term code to mean linear code as this paper only considers such codes. Elements of C are called codewords. A parity-check matrix for the code C is a matrix $H \in \mathbb{F}^{r\times n}$ such that C is the null space of H; that is, an element $\mathbf{y} \in \mathbb{F}^n$ is a codeword of C if and only if $H\mathbf{y}^T = \mathbf{0} \in \mathbb{F}^{r\times 1}$. Because a parity-check matrix of a code is not unique and the set of pseudocodewords depends on the choice of parity-check matrix, we use the notation $C(H)$ to emphasize that the code C is given by the parity-check matrix H; that is, given $H \in \mathbb{F}^{r\times n}$, the code with parity-check matrix H is

$$C(H) \coloneqq \left\{\mathbf{c} \in \mathbb{F}^n : H\mathbf{c}^T = \mathbf{0} \in \mathbb{F}^{r\times 1}\right\}.$$

Copyright (c) 2014 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TIT.2014.2331677

II. Preliminaries

Throughout, we assume that data is transmitted over a memoryless p-ary symmetric channel (though parts of the discussion in other sections apply more broadly). Given a code $C(H)$ over $\mathbb{F}_p$, one may associate with the parity-check matrix $H \in \mathbb{F}_p^{r\times n}$ a weighted bipartite graph called the Tanner graph of H. The Tanner graph of H, denoted $T(H)$, is a graph with biadjacency matrix H. Specifically, the vertex set of $T(H)$ is $X \cup F$ where $X = \{x_1, \ldots, x_n\}$ is the set of symbol nodes and $F = \{f_1, \ldots, f_r\}$ is the set of check nodes. If $h_{ji} \neq 0$, then $\{x_i, f_j\}$ is an edge with weight

$$w(x_i, f_j) \coloneqq h_{ji}.$$

Alternatively, one may think of the vertex x_i as corresponding to the i^{th} column of H, the vertex f_j as corresponding to the j^{th} row of H, and the edge $\{x_i, f_j\}$ as corresponding to the element h_{ji} of H. Notice that $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in \mathbb{F}_p^n$ is a codeword of $C(H)$ if and only if the assignment of the values $c_1, c_2, \ldots, c_n$ to their corresponding symbol nodes on the Tanner graph satisfies

$$\sum_{i:\, x_i \in \mathcal{N}(f_j)} w(x_i, f_j) \odot c_i = 0$$

for all j, $1 \leq j \leq r$, where the sum and the product are taken over $\mathbb{F}_p$ and $\mathcal{N}(f_j)$ denotes the set of vertices adjacent to f_j.

An m-cover of $T(H)$ is a weighted bipartite graph $\widetilde{G}$ such that there exists an m-to-one surjective mapping π from the vertices of $\widetilde{G}$ to the vertices of $T(H)$ where π preserves degree, and the image of adjacent vertices of $\widetilde{G}$ are adjacent in $T(H)$ with the same edge weight. For a vertex $v_i \in X \cup F$, the vertices in the set $\pi^{-1}(v_i)$ are called *copies* of v_i and are denoted $v_{(i,1)}, v_{(i,2)}, \ldots, v_{(i,m)}$. Let $C(\widetilde{G})$ denote the code of length mn over $\mathbb{F}_p$ defined by an m-cover $\widetilde{G}$. We write the codeword $\tilde{\mathbf{c}} \in C(\widetilde{G})$ as

$$\tilde{\mathbf{c}} = \left(\tilde{c}_{(1,1)}, \ldots, \tilde{c}_{(1,m)}, \ldots, \tilde{c}_{(n,1)}, \ldots, \tilde{c}_{(n,m)}\right).$$

For each $b \in \mathbb{F}_p^*$ and $1 \leq i \leq n$, let

$$m_i(b) \coloneqq |\{1 \leq l \leq m : \tilde{c}_{(i,l)} = b\}|;$$

i.e., $m_i(b)$ is the number of copies of the symbol node x_i that take value $b \in \mathbb{F}_p$. Thus, for each $i = 1, \ldots, n$, one may associate the values assigned to the copies of the i^{th} symbol node, meaning $\tilde{c}_{(i,1)}, \ldots, \tilde{c}_{(i,m)}$, with a column vector

$$\begin{bmatrix} m_i(1) \\ \vdots \\ m_i(p-1) \end{bmatrix}.$$

As a result, each codeword

$$\tilde{\mathbf{c}} = (\underbrace{\tilde{c}_{(1,1)}, \ldots, \tilde{c}_{(1,m)}}_{\begin{bmatrix} m_1(1) \\ \vdots \\ m_1(p-1) \end{bmatrix}}, \underbrace{\tilde{c}_{(2,1)}, \ldots, \tilde{c}_{(2,m)}}_{\begin{bmatrix} m_2(1) \\ \vdots \\ m_2(p-1) \end{bmatrix}}, \ldots, \underbrace{\tilde{c}_{(n,1)} \ldots \tilde{c}_{(n,m)}}_{\begin{bmatrix} m_n(1) \\ \vdots \\ m_n(p-1) \end{bmatrix}})$$

of $C(\widetilde{G})$ defines a *graph cover pseudocodeword* (more precisely, an *unscaled graph cover pseudocodeword*), written in matrix form as

$$\mathcal{M} \coloneqq \begin{bmatrix} m_1(1) & m_2(1) & \cdots & m_n(1) \\ \vdots & \vdots & & \vdots \\ m_1(p-1) & m_2(p-1) & \cdots & m_n(p-1) \end{bmatrix}$$

in $\mathbb{N}^{(p-1)\times n}$. Note that $\mathrm{Row}_b(\mathcal{M})$ corresponds to an element $b \in \mathbb{F}_p^*$. Thus, one may abuse the notation and regard the indices of the rows of $\mathcal{M}$ as elements of $\mathbb{F}_p^*$. This is particularly useful in the following expression. If $\tilde{\mathbf{c}}$ is a codeword of $C(\widetilde{G})$, then

$${}^a\tilde{\mathbf{c}} \coloneqq \left(a \odot \tilde{c}_{(1,1)}, \ldots, a \odot \tilde{c}_{(n,m)}\right)$$

is also a codeword of $C(\widetilde{G})$ for all $a \in \mathbb{F}_p$. The resulting pseudocodeword matrix, denoted ${}^a\mathcal{M}$, can be obtained by permuting rows of $\mathcal{M}$; specifically, for all $1 \leq b \leq p-1$ and $a \in \mathbb{F}_p^*$,

$$\mathrm{Row}_{b\odot a}({}^a\mathcal{M}) = \mathrm{Row}_b(\mathcal{M}).$$

One may also write a graph cover pseudocodeword in vector form as

$$\mathbf{m} \coloneqq (m_1(1), \ldots, m_n(1), \ldots, m_1(p-1), \ldots, m_n(p-1)) \in \mathbb{N}^{(p-1)n}.$$

Notice that

$$\mathcal{M}(\mathbf{m}) = \mathcal{M}$$

where the map $\mathcal{M} : \mathbb{N}^{(p-1)n} \to \mathbb{N}^{(p-1)\times n}$ is defined by

$$\mathcal{M}(\mathbf{v}) \coloneqq \begin{bmatrix} v_1 & v_2 & \cdots & v_n \\ v_{n+1} & v_{n+2} & \cdots & v_{2n} \\ \vdots & \vdots & & \vdots \\ v_{(p-2)n+1} & v_{(p-2)n+2} & \cdots & v_{(p-1)n} \end{bmatrix}.$$

The associated *normalized graph cover pseudocodeword* is

$$\frac{\mathcal{M}}{m} \in [0,1]^{(p-1)\times n}$$

in matrix form and

$$\frac{\mathbf{m}}{m} \in [0,1]^{(p-1)n}$$

Copyright (c) 2014 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TIT.2014.2331677

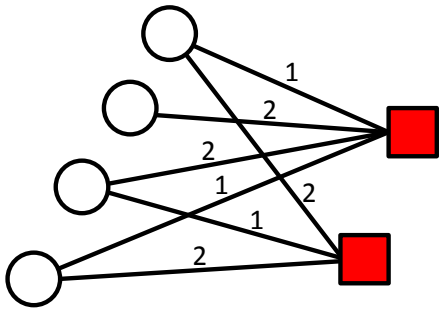

Fig. 1. The Tanner graph $T(H)$ from Example 2.1.

in vector form, respectively. Henceforth, we use the term pseudocodeword to mean graph cover pseudocodeword. Given $H \in \mathbb{F}_p^{r\times n}$, let

$$\mathcal{PC}(H) := \left\{ \mathbf{m} \in \mathbb{N}^{(p-1)n} : \begin{array}{l} \mathbf{m} \text{ is a pseudo-} \\ \text{codeword of } C(H) \end{array} \right\}$$

denote the set of pseudocodewords of H; note that $\mathbf{m} \in \mathcal{PC}(H)$ if and only if there exists a positive integer m such that $\mathbf{m}$ is a pseudocodeword coming from an m-cover of $T(H)$.

Example 2.1: Consider the ternary code $C(H)$ given by

$$H = \begin{bmatrix} 1 & 2 & 2 & 1 \\ 2 & 0 & 1 & 2 \end{bmatrix} \in \mathbb{F}_3^{2\times 4}.$$

Note that this parity-check matrix was considered in [22]. Then, $C(H)$ is a code over $\mathbb{F}_3$ of length 4 and dimension 2. The codewords of $C(H)$ are $(0,0,0,0)$, $(0,0,1,1)$, $(0,0,2,2)$, $(1,0,0,2)$, $(2,0,0,1)$, $(1,0,1,0)$, $(2,0,2,0)$, $(1,0,2,1)$, and $(2,0,1,2)$. Here, Figure 1 illustrates the Tanner graph $T(H)$, and Figure 2 shows a 4-cover of $T(H)$, and the codeword

$$\tilde{\mathbf{c}} = (2,0,2,1,0,1,1,1,2,1,1,0,0,2,0,0)$$

on $\widetilde{G}$. Thus, the pseudocodeword matrix $\mathcal{M}$ and its vector form $\mathbf{m}$ are

$$\mathcal{M} = \begin{bmatrix} 1 & 3 & 2 & 0 \\ 2 & 0 & 1 & 1 \end{bmatrix}$$

and

$$\mathbf{m} = (1,3,2,0,2,0,1,1)$$

respectively.

The terminology for nonbinary pseudocodewords given thus far coincides with that generally accepted in

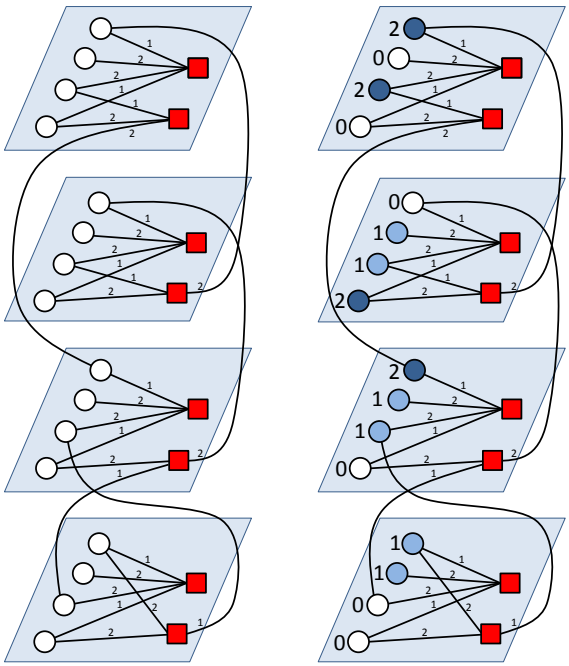

Fig. 2. A 4-cover $\widetilde{G}$ and the codeword $(2,0,2,1,0,1,1,1,2,1,1,0,0,2,0,0)$ of $C(\widetilde{G})$ from Example 2.1.

the binary case. In particular, let $H \in \mathbb{F}_2^{r\times n}$ and $\widetilde{G}$ be an m-cover of $T(H)$. Given a codeword

$$\left(\tilde{c}_{(1,1)}, \ldots, \tilde{c}_{(1,m)}, \ldots, \tilde{c}_{(n,1)} \cdots \tilde{c}_{(n,m)}\right) \in C(\widetilde{G}),$$

the pseudocodeword matrix and its vector form are

$$\mathcal{M} = \begin{bmatrix} m_1(1) & m_2(1) & \cdots & m_n(1) \end{bmatrix} \in \mathbb{N}^{1\times n}$$

and

$$\mathbf{m} = (m_1(1), m_2(1), \ldots, m_n(1)) \in \mathbb{N}^n$$

respectively. On the other hand, the associated graph cover pseudocodeword in the binary sense is

$$\mathbf{p} := (p_1, p_2, \ldots, p_n).$$

where $p_i = \sum_{l=1}^{m} \tilde{c}_{(i,l)}$. Here, it follows that

$$\mathcal{M} = \mathbf{m} = \mathbf{p}$$

since

$$m_i(1) = |\{1 \le l \le m \mid \tilde{c}_{(i,l)} = 1\}| = \sum_{l=1}^{m} \tilde{c}_{(i,l)} = p_i.$$

Alternatively, one may define graph cover pseudocodewords from the linear programming decoding perspective [8], [24]. To do so, define

$$\begin{array}{rccc} \phi: & \mathbb{F}_p^n & \to & \{0,1\}^{(p-1)n} \\ & \mathbf{x} & \mapsto & (\mathbf{e}_{x_1}, \mathbf{e}_{x_2}, \ldots, \mathbf{e}_{x_n}) \end{array}$$

Copyright (c) 2014 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TIT.2014.2331677

where $\mathbf{e}_0$ is the all-zero vector and $\mathbf{e}_i \in \{0,1\}^{p-1}$ denotes the standard basis vector with 1 in the i^{th} coordinate and zeros elsewhere. The codeword polytope of $C(H) \subseteq \mathbb{F}_p^n$ is

$$poly(C(H)) \coloneqq \left\{ \sum_{\mathbf{c}\in C(H)} \lambda_{\mathbf{c}} \phi(\mathbf{c}) : \begin{array}{l} \sum_{\mathbf{c}\in C(H)} \lambda_{\mathbf{c}} = 1, \\ \lambda_{\mathbf{c}} \geq 0 \end{array} \right\} \subseteq [0,1]^{(p-1)n}.$$

Given a received word $\mathbf{y}$, maximum-likelihood decoding is equivalent to

$$\text{minimize} \sum_{k=1}^{(p-1)n} \gamma_k f_k \text{ subject to } \mathbf{f} \in poly(C(H))$$

where

$$\gamma_{(p-1)(i-1)+a} = \log\left(\frac{P(y_i \mid 0)}{P(y_i \mid a)}\right)$$

for all $i = 1,\ldots,n$ and $a = 1,\ldots,p-1$. The fundamental polytope of $H \in \mathbb{F}_p^{r\times n}$ is

$$Q(H) \coloneqq \cap_{j=1}^{r} poly\left(C\left(\text{Row}_j(H)\right)\right).$$

Note that

$$poly(C(H)) \subseteq Q(H).$$

Linear code LP decoding is

$$\text{minimize} \sum_{k=1}^{(p-1)n} \gamma_k f_k \text{ subject to } \mathbf{f} \in Q(H).$$

Since $poly(C(H)) \subseteq Q(H)$, LP decoding is easily seen as a relaxation of maximum-likelihood decoding whose benefit is the reduction in the number of inequalities used to define the feasible region. However, this relaxation may lead to a noncodeword output; such words together with the codewords are called normalized LP pseudocodewords [8, Theorem 6.1].

The relationship between LP pseudocodewords and graph cover pseudocodewords is described as follows by Flanagan et al. [8, Corollary 7.2] (see also [26] for the binary case). There exists a graph cover pseudocodeword with a (normalized) pseudocodeword matrix $\mathcal{M}$ if and only if there exists a (normalized) LP pseudocodeword $\mathbf{v}$ with $\mathcal{M}(\mathbf{v}) = \mathcal{M}$.

In the next section, we examine the fundamental cone, which is the conic hull of the fundamental polytope. The description of the fundamental cone can be simpler than that of the fundamental polytope while encapsulating the information relevant to pseudocodewords. There are various descriptions of the fundamental polytope, and it is yet to be determined which among them is the most convienient for LP decoder implementation and its analysis. For instance, the recent works [12] and [21] only utilize the fundamental polytope description implicitly.

III. Pseudocodewords of codes over $\mathbb{F}_p$

A. Toward inequalities defining the fundamental cone

In this section, we provide bounds that p-ary pseudocodewords satisfy. We begin by introducing the notion of a *critical multiset* which is key in producing these bounds.

Definition 3.1: A critical multiset of order p is a multiset $\{\gamma_1,\ldots,\gamma_t\} \subseteq \{0,1,\ldots,p-1\}$ where $t \geq 2$ and

$$\sum_{i=1}^{t} \gamma_i > (t-1)p.$$

For convenience, we refer to the critical multisets of order p as critical multisets of $\mathbb{F}_p$. The set of critical multisets of $\mathbb{F}_p$ is denoted Γ_p.

Example 3.2: The critical multisets of $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_5$, and $\mathbb{F}_7$ are as follows:

- $\Gamma_2 = \emptyset$,
- $\Gamma_3 = \{\{2,2\}\}$,
- $\Gamma_5 = \{\{2,4\},\{3,3\},\{3,4\},\{4,4\},$ $\{3,4,4\},\{4,4,4\},\{4,4,4,4\}\}$, and
- $\Gamma_7 = \{\{2,6\},\{3,5\},\{3,6\},\{4,4\},\{4,5\},$ $\{4,6\},\{5,5\},\{5,6\},\{6,6\},$ $\{3,6,6\},\{4,5,6\},\{4,6,6\},\{5,5,5\},$ $\{5,5,6\},\{5,6,6\},\{6,6,6\},$ $\{4,6,6,6\},\{5,5,6,6\},\{5,6,6,6\},$ $\{6,6,6,6\},\{5,6,6,6,6\},$ $\{6,6,6,6,6,6\},\{6,6,6,6,6,6,6\}\}$.

Example 3.3: In this example, we consider critical mulitsets of $\mathbb{F}_p$. The only critical multiset of cardinality $p-1$ is $\{p-1,\ldots,p-1\}$. The critical multisets of cardinality $p-2$, where $p \geq 5$, are $\{p-1,\ldots,p-1\}$ and $\{p-2,p-1,\ldots,p-1\}$. The critical multisets of $\mathbb{F}_p$ of cardinality $p-3$, where $p \geq 5$, are $\{p-2,p-2,p-1,\ldots,p-1\}$, $\{p-3,p-1,\ldots,p-1\}$, $\{p-2,p-1,\ldots,p-1\}$ and $\{p-1,\ldots,p-1\}$. The multiset $\{a,p-a+1\}$ is critical for all a, $2 \leq a \leq p-1$.

Proposition 3.4: A multiset $\{\gamma_1,\ldots,\gamma_t\} \subseteq \mathbb{F}_p$ is critical if and only if $\{p-\gamma_1,\ldots,p-\gamma_t\}$ is a partition of a number less than p with at least 2 parts.

Proof It follows from the definition of critical multiset that

$$\sum_{i=1}^{t} p - \gamma_i < p.$$

Copyright (c) 2014 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TIT.2014.2331677

■

Corollary 3.5: If a multiset $\{\gamma_1, \ldots, \gamma_t\} \subseteq \mathbb{F}_p$ is critical, then any multisubset of $\{\gamma_1, \ldots, \gamma_t\}$ of cardinality greater than 1 is critical. Furthermore,

$$\sum_{i=1}^{t} \gamma_i \neq 0 \mod p.$$

Let Γ_p^* denote the set of critical multisets A of $\mathbb{F}_p$ that are not proper multisubsets of any critical multiset of $\mathbb{F}_p$; we refer to such a multiset as a *maximal critical multiset*. In light of the previous corollary, it is useful to have a characterization of maximal critical multisets. The next corollary follows immediately from Proposition 3.4.

Corollary 3.6: A multiset $\{\gamma_1, \ldots, \gamma_t\} \subseteq \mathbb{F}_p$ is a maximal critical multiset of $\mathbb{F}_p$ if and only if $\{p - \gamma_1, \ldots, p - \gamma_t\}$ is a partition of $p-1$ with at least 2 parts. Hence, the number of maximal critical multisets of order p is $\mid \Gamma_p^* \mid = P(p-1) - 1$ where $P(n)$ denotes the partition number of an integer n.

Example 3.7: The maximal critical multisets of $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_5$, and $\mathbb{F}_7$ are as follows:

- $\Gamma_2^* = \Gamma_2 = \emptyset$,
- $\Gamma_3^* = \Gamma_3 = \{\{2,2\}\}$,
- $\Gamma_5^* = \{\{2,4\},\{3,3\},\{3,4,4\},\{4,4,4,4\}\}$, and
- $\Gamma_7^* = \{\{2,6\},\{3,5\},\{4,4\},\{3,6,6\},\{4,5,6\},$ $\{5,5,5\},\{4,6,6,6\},\{5,5,6,6\},$ $\{5,6,6,6,6\},\{6,6,6,6,6,6\}\}$.

To provide conditions that pseudocodewords of codes over $\mathbb{F}_p$ must satisfy, it is natural to relate pseudocodewords to real numbers. We will see that the real numbers corresponding to pseudocodewords are bounded below by sums involving critical multisets.

Let $H \in \mathbb{F}_p^{r \times n}$ and $\widetilde{G}$ be an m-cover of $T(H)$. Given a codeword

$$\tilde{\mathbf{c}} = \left(\tilde{c}_{(1,1)}, \ldots, \tilde{c}_{(1,m)}, \ldots, \tilde{c}_{(n,1)}, \ldots, \tilde{c}_{(n,m)}\right)$$

of $C(\widetilde{G})$, we quantify the weighted sum of the neighbors of every copy of the j^{th} check node in the following definition.

Definition 3.8: Let $H \in \mathbb{F}_p^{r \times n}$. Given $1 \leq j \leq r$ and a pseudocodeword matrix $\mathcal{M} \in \mathbb{Z}^{(p-1) \times n}$ of $C(H)$, define

$$\Theta_j(\mathcal{M}) \coloneqq \frac{1}{p} \sum_{b=1}^{p-1} \Big(b \odot \operatorname{Row}_j(H)\Big) \operatorname{Row}_b(\mathcal{M})^T \quad (1)$$

where the product $b \odot \operatorname{Row}_j(H)$ is taken in $\mathbb{F}_p$ and the inner product $\Big(b \odot \operatorname{Row}_j(H)\Big) \operatorname{Row}_b(\mathcal{M})^T$ and the sum are taken in $\mathbb{R}$.

Proposition 3.9: Let $C(H)$ be the code given by a parity-check matrix $H \in \mathbb{F}_p^{r \times n}$ and let $\mathcal{M}$ be a pseudocodeword matrix of $C(H)$ corresponding to a codeword $\tilde{\mathbf{c}}$ of $C(\widetilde{G})$. Then,

$$\Theta_j(\mathcal{M}) = \frac{1}{p} \sum_{\substack{1 \leq l \leq m \\ i \in \operatorname{supp}(\operatorname{Row}_j(H))}} w(x_i, f_j) \odot \tilde{c}_{(i,l)}$$

for all $1 \leq j \leq r$, where the sum is taken in $\mathbb{R}$ and $\tilde{G}$ is an m-cover.

Proof We have

$$\begin{aligned}
\Theta_j(\mathcal{M}) &= \frac{1}{p} \sum_{b=1}^{p-1} \Big(b \odot \operatorname{Row}_j(H)\Big) \operatorname{Row}_b(\mathcal{M})^T \\
&= \frac{1}{p} \sum_{b=1}^{p-1} \sum_{i=1}^{n} \Big(b \odot h_{ji}\Big) m_i(b) \\
&= \frac{1}{p} \sum_{i=1}^{n} \sum_{b=1}^{p-1} \sum_{\{l \mid \tilde{c}_{(i,l)} = b\}} b \odot h_{ji} \\
&= \frac{1}{p} \sum_{i=1}^{n} \sum_{l=1}^{m} h_{ji} \odot \tilde{c}_{(i,l)}
\end{aligned}$$

where the summations throughout are taken in $\mathbb{R}$. The desired result follows since $h_{ji} = 0$ if $i \notin \operatorname{supp}(\operatorname{Row}_j(H))$ and $h_{ji} = w(x_i, f_j)$ otherwise. ■

Notice that the definition of Θ given in (1) involves only the parity-check matrix H and pseudocodeword matrix $\mathcal{M}$. However, Proposition 3.9 implies that $\Theta_j(\mathcal{M})$ is equal to a weighted sum of $w(x_i, f_j) \odot \tilde{c}_{(i,l)}$ over all $1 \leq l \leq m$ and $i \in \operatorname{supp}(\operatorname{Row}_j(H))$. Therefore, $\Theta_j(\mathcal{M})$ captures an attribute of $\tilde{\mathbf{c}}$ without explicit knowledge of $\tilde{\mathbf{c}}$ and the particular graph cover $\widetilde{G}$, where $\tilde{\mathbf{c}} \in C(\widetilde{G})$.

Recall that ${}^a\mathcal{M}$ is a pseudocodeword matrix obtained as a multiple of $\mathcal{M}$. The following corollary gives a similar identity for $\Theta_j({}^a\mathcal{M})$.

Corollary 3.10: Let $C(H)$ be the code given by a parity-check matrix $H \in \mathbb{F}_p^{r \times n}$ and let $\mathcal{M}$ be a pseudocodeword matrix of $C(H)$ corresponding to a codeword $\tilde{\mathbf{c}}$ of $C(\widetilde{G})$. If $a \in \mathbb{F}_p^*$, then

$$\Theta_j({}^a\mathcal{M}) = \frac{1}{p} \sum_{\substack{1 \leq l \leq m \\ i \in \operatorname{supp}(\operatorname{Row}_j(H))}} a \odot w(x_i, f_j) \odot \tilde{c}_{(i,l)}$$

for all $1 \leq j \leq r$, where the sum is taken in $\mathbb{R}$ and $\tilde{G}$ is an m-cover .

Next, we develop a set of bounds that all pseudocodewords of a code over $\mathbb{F}_p$ must satisfy.

Theorem 3.11: Consider a parity-check matrix $H \in \mathbb{F}_p^{r \times n}$ where p is prime. Let $\mathcal{M}$ be a pseudocodeword matrix of $C(H)$. Then, for all

Copyright (c) 2014 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TIT.2014.2331677

$1 \le j \le r$, $\mathcal{M}$ must satisfy all of the following conditions.

Column sum bound: For all $a \in \mathbb{F}_p^*$ and $i \in \operatorname{supp}(\operatorname{Row}_j(H))$,

$$\Theta_j({}^a\mathcal{M}) \ge m_i(1) + m_i(2) + \cdots + m_i(p-1). \quad (2)$$

Critical multiset bound: For all $a \in \mathbb{F}_p^*$, distinct $i_1, \ldots, i_t \in \operatorname{supp}(\operatorname{Row}_j(H))$, and maximal critical multisets $\{\gamma_1, \ldots, \gamma_t\} \in \Gamma_p^*$,

$$\Theta_j({}^a\mathcal{M}) \ge \sum_{s=1}^{t} m_{i_s}\left(\gamma_s \odot a^{-1} \odot h_{ji_s}^{-1}\right). \quad (3)$$

Parity condition:

$$H\mathcal{M}^T \begin{bmatrix} 1 \\ 2 \\ \vdots \\ p-1 \end{bmatrix} \mod p = \mathbf{0}. \quad (4)$$

Nonnegativity condition: For all $i \in \operatorname{supp}(\operatorname{Row}_j(H))$ and $b \in \mathbb{F}_p^*$,

$$m_i(b) \ge 0. \quad (5)$$

Proof Given a pseudocodeword matrix $\mathcal{M}$, there exists a graph cover $\widetilde{G}$ of the Tanner graph of H such that $\mathcal{M}$ corresponds to a codeword

$$\tilde{\mathbf{c}} = (\tilde{c}_{(1,1)}, \ldots, \tilde{c}_{(1,m)}, \ldots, \tilde{c}_{(n,1)}, \ldots, \tilde{c}_{(n,m)})$$

of $C(\widetilde{G})$. To express the parity condition enforced by copies of the check node f_j on the graph cover $\widetilde{G}$, we will first fix a labeling of the symbol node. Let $1 \le j \le r$. For each $i \in \operatorname{supp}(\operatorname{Row}_j(H))$, label the vertices of $\widetilde{G}$ such that if the weight of the edge $\{x_i, f_j\}$ of the Tanner graph of H is w (equivalently, if $h_{ji} = w$), then $\{x_{(i,l)}, f_{(j,l)}\}$ is an edge of $\widetilde{G}$ with weight w. In other words, we index copies of each neighbor of f_j using the indices of copies of f_j in $\widetilde{G}$. This is possible because adjacency is preserved in the graph cover; however, this naming convention is dependent on j. (In effect, giving such labeling for all j at the same time may not be possible. This does not present a problem here, because the statements in the theorem do not depend on the index of the symbol node.) Now, for each $1 \le l \le m$, we can express the parity condition at the l^{th} copy of f_j as

$$\sum_{i \in \operatorname{supp}(\operatorname{Row}_j(H))} w(x_i, f_j) \odot \tilde{c}_{(i,l)} \mod p = 0. \quad (6)$$

Here and throughout, the summation is taken in $\mathbb{R}$.

To prove (2), we fix $i \in \operatorname{supp}(\operatorname{Row}_j(H))$ and count the number of nonzero copies of x_i in $\tilde{\mathbf{c}}$; that is, we consider

$$\mathscr{A} := \left\{1 \le l \le m \mid \tilde{c}_{(i,l)} \ne 0\right\}.$$

It is clear that

$$|\mathscr{A}| = m_i(1) + m_i(2) + \cdots + m_i(p-1).$$

Now, if $\tilde{c}_{(i,l)} \ne 0$, then

$$w(x_i, f_j) \odot \tilde{c}_{(i,l)} \ne 0$$

since $i \in \operatorname{supp}(\operatorname{Row}_j(H))$ and $w(x_i, f_j) = h_{ji} \ne 0$. It follows from (6) that

$$\sum_{i' \in \operatorname{supp}(\operatorname{Row}_j(H))} w(x_{i'}, f_j) \odot \tilde{c}_{(i',l)}$$

is a nonzero multiple of p if $\tilde{c}_{(i,l)} \ne 0$. The fact that $w(x_i, f_j) \odot \tilde{c}_{(i,l)} \ne 0$ also implies that

$$\sum_{i' \in \operatorname{supp}(\operatorname{Row}_j(H))} a \odot w(x_{i'}, f_j) \odot \tilde{c}_{(i',l)}$$

is a nonzero multiple of p for any $a \in \mathbb{F}_p^*$. Therefore,

$$\sum_{i' \in \operatorname{supp}(\operatorname{Row}_j(H))} a \odot w(x_{i'}, f_j) \odot \tilde{c}_{(i',l)} \ge p$$

for l, $1 \le l \le m$, with $\tilde{c}_{(i,l)} \ne 0$. Applying Corollary 3.10, we conclude that

$$\begin{aligned}
&\Theta_j({}^a\mathcal{M}) \\
&= \frac{1}{p} \sum_{1 \le l \le m} \sum_{i' \in \operatorname{supp}(\operatorname{Row}_j(H))} a \odot w(x_{i'}, f_j) \odot \tilde{c}_{(i',l)} \\
&\ge \frac{1}{p} \sum_{\substack{1 \le l \le m \\ \tilde{c}_{(i,l)} \ne 0}} p \\
&= \sum_{\substack{1 \le l \le m \\ \tilde{c}_{(i,l)} \ne 0}} 1 \\
&= |\mathscr{A}| \\
&= m_i(1) + m_i(2) + \cdots + m_i(p-1).
\end{aligned}$$

Next, we prove (3) for $a = 1$. Fix $i_1, \ldots, i_t \in \operatorname{supp}(\operatorname{Row}_j(H))$ and $\{\gamma_1, \ldots, \gamma_t\} \in \Gamma_p^*$. Note that $h_{ji_s}^{-1}$ exists for all $1 \le s \le t$ since $i_1, \ldots, i_t \in \operatorname{supp}(\operatorname{Row}_j(H))$. Consider

$$\mathscr{B} := \left\{(s,l) : \begin{array}{l} w(x_{i_s}, f_j) \odot \tilde{c}_{(i_s,l)} = \gamma_s, \\ 1 \le s \le t \text{ and } 1 \le l \le m \end{array}\right\}.$$

For each s,

$$w(x_{i_s}, f_j) \odot \tilde{c}_{(i_s,l)} = \gamma_s$$

Copyright (c) 2014 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TIT.2014.2331677

if and only if

$$\begin{aligned}\tilde{c}_{(i_s,l)} &= \gamma_s \odot w(x_{i_s}, f_j)^{-1} \\ &= \gamma_s \odot h_{ji_s}^{-1}.\end{aligned}$$

Thus,

$$|\mathscr{B}| = m_{i_1}\left(\gamma_1 \odot h_{ji_1}^{-1}\right) + \cdots + m_{i_t}\left(\gamma_t \odot h_{ji_t}^{-1}\right).$$

For each l, let

$$\begin{aligned}\mathscr{B}(l) &\coloneqq \{s \mid (s,l) \in \mathscr{B}\} \\ &= \left\{1 \le s \le t \mid w(x_{i_s}, f_j) \odot \tilde{c}_{(i_s,l)} = \gamma_s\right\}.\end{aligned}$$

Then,

$$\begin{aligned}&\sum_{i' \in \operatorname{supp}(\operatorname{Row}_j(H))} w(x_{i'}, f_j) \odot \tilde{c}_{(i',l)} \\ &\qquad \ge \sum_{s \in \mathscr{B}(l)} w(x_{i_s}, f_j) \odot \tilde{c}_{(i_s,l)} \\ &\qquad = \sum_{s \in \mathscr{B}(l)} \gamma_s \\ &\qquad > (|\mathscr{B}(l)| - 1)p.\end{aligned} \tag{7}$$

To verify the last inequality, we consider the cases $|\mathscr{B}(l)| = 0$, $|\mathscr{B}(l)| = 1$, and $|\mathscr{B}(l)| \ge 2$. If $|\mathscr{B}(l)| = 0$, then clearly $\sum_{s \in \mathscr{B}(l)} \gamma_s = 0 > -p$. If $|\mathscr{B}(l)| = 1$, then $\sum_{s \in \mathscr{B}(l)} \gamma_s = \gamma_s$ for some s. Since $\{\gamma_1, \ldots, \gamma_t\}$ is a critical multiset, $\gamma_s > 0 = (|\mathscr{B}(l)| - 1)p$. In the case $|\mathscr{B}(l)| \ge 2$ Corollary 3.5 applies, and $\sum_{s \in \mathscr{B}(l)} \gamma_s > (|\mathscr{B}(l)| - 1)p$ as $\mathscr{B}(l)$ is a critical multiset. Now, it follows from (6) and (7) that

$$\sum_{i' \in \operatorname{supp}(\operatorname{Row}_j(H))} w(x_{i'}, f_j) \odot \tilde{c}_{(i',l)}$$

is a multiple of p that is larger than $(|\mathscr{B}(l)| - 1)p$. Thus,

$$\sum_{i' \in \operatorname{supp}(\operatorname{Row}_j(H))} w(x_{i'}, f_j) \odot \tilde{c}_{(i',l)} \ge |\mathscr{B}(l)|p.$$

We now apply Proposition 3.9 to obtain

$$\begin{aligned}\Theta_j(\mathcal{M}) &= \frac{1}{p} \sum_{1 \le l \le m} \sum_{i' \in \operatorname{supp}(\operatorname{Row}_j(H))} w(x_{i'}, f_j) \odot \tilde{c}_{(i',l)} \\ &\ge \frac{1}{p} \sum_{1 \le l \le m} |\mathscr{B}(l)|p \\ &= |\mathscr{B}| \\ &= m_{i_1}\left(\gamma_1 \odot h_{ji_1}^{-1}\right) + \cdots + m_{i_t}\left(\gamma_t \odot h_{ji_t}^{-1}\right).\end{aligned}$$

This completes the proof of (3) when $a = 1$. For $a \in \mathbb{F}_p^*$ we recall that $\operatorname{Row}_j({}^a\mathcal{M}) = \operatorname{Row}_{j \odot a^{-1}}(\mathcal{M})$ and apply the above bound to ${}^a\mathcal{M}$ to obtain

$$\Theta_j({}^a\mathcal{M}) \ge \sum_{s=1}^{t} m_{i_s}\left(\gamma_s \odot a^{-1} \odot h_{ji_s}^{-1}\right)$$

as desired.

Condition (5) is trivial as

$$m_i(b) = |\{1 \le l \le m \mid \tilde{c}_{(i,l)} = b\}|.$$

We are now left to show that (4) holds. Recall from (1) that

$$p\,\Theta_j(\mathcal{M}) = \sum_{b=1}^{p-1} \Big(b \odot \operatorname{Row}_j(H)\Big) \operatorname{Row}_b(\mathcal{M})^T.$$

Thus,

$$\begin{aligned}&p\,\Theta_j(\mathcal{M}) \mod p \\ &= \sum_{b=1}^{p-1} \Big(b \odot \operatorname{Row}_j(H)\Big) \operatorname{Row}_b(\mathcal{M})^T \mod p \\ &= \operatorname{Row}_j(H)\mathcal{M}^T \begin{bmatrix} 1 \\ 2 \\ \vdots \\ p-1 \end{bmatrix} \mod p.\end{aligned} \tag{8}$$

On the other hand, applying Proposition 3.9 and Equation (6) yields

$$\begin{aligned}&p\,\Theta_j(\mathcal{M}) \mod p \\ &= \sum_{1 \le l \le m} \sum_{i' \in \operatorname{supp}(\operatorname{Row}_j(H))} w(x_{i'}, f_j) \odot \tilde{c}_{(i',l)} \mod p \\ &= 0.\end{aligned} \tag{9}$$

Combining (8) and (9) yields

$$\operatorname{Row}_j(H)\mathcal{M}^T \begin{bmatrix} 1 \\ 2 \\ \vdots \\ p-1 \end{bmatrix} \mod p = 0$$

for all $1 \le j \le r$, and Equation (4) follows. ∎

A corollary to Theorem 3.11 is the next result obtained by Skachek and Flanagan.

Corollary 3.12: [23, Theorem 3.1] Let $H \in \mathbb{F}_p^{r \times n}$. If $\mathcal{M}$ is a pseudocodeword of $C(H)$, then

$$\sum_{\substack{i' \in \operatorname{supp}(\operatorname{Row}_j(H)) \setminus \{i\} \\ b \in \mathbb{F}_p^*}} m_{i'}(b) \ge \sum_{b \in \mathbb{F}_p^*} m_i(b)$$

for all $1 \le j \le r$ and $i \in \operatorname{supp}(\operatorname{Row}_j(H))$.

Proof We sum Equation (2) from Theorem 3.11 over all $a \in \mathbb{F}_p^*$ to obtain

$$\sum_{a \in \mathbb{F}_p^*} \Theta_j({}^a\mathcal{M}) \ge \sum_{a \in \mathbb{F}_p^*} m_i(1) + m_i(2) + \cdots + m_i(p-1).$$

Copyright (c) 2014 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TIT.2014.2331677

Applying Corollary 3.10 yields

$$\begin{aligned}
&\sum_{a\in\mathbb{F}_p^*} \Theta_j({}^a\mathcal{M}) \\
&= \sum_{a\in\mathbb{F}_p^*} \frac{1}{p} \sum_{\substack{1\le l\le m \\ i'\in \mathrm{supp}(\mathrm{Row}_j(H))}} a\odot w(x_{i'},f_j)\odot \tilde{c}_{(i',l)} \\
&= \frac{1}{p} \sum_{\substack{1\le l\le m \\ i'\in \mathrm{supp}(\mathrm{Row}_j(H))}} \left(\sum_{a\in\mathbb{F}_p^*} a\odot w(x_{i'},f_j)\odot \tilde{c}_{(i',l)} \right) \\
&= \frac{1}{p} \sum_{\left\{\tilde{c}_{(i',l)}\neq 0 :\ \substack{1\le l\le m, \\ i'\in \mathrm{supp}(\mathrm{Row}_j(H))}\right\}} \frac{p(p-1)}{2} \\
&= \frac{p-1}{2} \left| \left\{ \tilde{c}_{(i',l)}\neq 0 :\ \substack{1\le l\le m, \\ i'\in \mathrm{supp}(\mathrm{Row}_j(H))} \right\} \right| \\
&= \frac{p-1}{2} \sum_{\substack{i'\in \mathrm{supp}(\mathrm{Row}_j(H)) \\ b\in\mathbb{F}_p^*}} m_{i'}(b).
\end{aligned}$$

On the other hand,

$$\begin{aligned}
&\sum_{a\in\mathbb{F}_p^*} m_i(1)+m_i(2)+\cdots+m_i(p-1) \\
&\qquad = (p-1)(m_i(1)+m_i(2)+\cdots+m_i(p-1)) \\
&\qquad = (p-1)\sum_{b\in\mathbb{F}_p^*} m_i(b).
\end{aligned}$$

We now have

$$\frac{p-1}{2} \sum_{\substack{i'\in \mathrm{supp}(\mathrm{Row}_j(H)) \\ b\in\mathbb{F}_p^*}} m_{i'}(b) \ge (p-1)\sum_{b\in\mathbb{F}_p^*} m_i(b),$$

and the desired result follows. ∎

Remark 3.13: The total number of inequalities in Theorem 3.11 is linear in n if the parity-check matrix H is sparse and $n \gg p$. In particular, the number of column sum bounds is $p\delta(H)$, where $\delta(H)$ is the number of nonzero entries of H (equivalently, the number of edges of the Tanner graph). It follows from Corollary 3.6 that the number of critical multiset bounds in Theorem 3.11 is exponential in p.

The bounds from Theorem 3.11 can be roughly interpreted in the following manner. We keep the notation consistent with the proof of the theorem: let us fix j and label the vertices of $\widetilde{G}$ so that $\{x_{(i,l)}, f_{(j,l)}\}$ is an edge of $\widetilde{G}$ with weight $w(x_i, f_j)$, and assume that $\tilde{\mathbf{c}} = (\tilde{c}_{(1,1)},\ldots,\tilde{c}_{(1,m)},\ldots,\tilde{c}_{(n,1)},\ldots,\tilde{c}_{(n,m)})$ is a codeword of $C(\widetilde{G})$. Column sum bounds guarantee that if $\tilde{c}_{(i,l)} \neq 0$ where $i \in \mathrm{supp}(\mathrm{Row}_j(H))$, then $\tilde{c}_{(i',l)} \neq 0$ for some $i' \in \mathrm{supp}(\mathrm{Row}_j(H)) \setminus \{i\}$. Critical multiset bounds consider the case when $h_{ji_1}\odot\tilde{c}_{(i_1,l)}, h_{ji_2}\odot\tilde{c}_{(i_2,l)},\ldots,h_{ji_t}\odot\tilde{c}_{(i_t,l)}$ take values from critical multiset $\{\gamma_1,\ldots,\gamma_t\}$. Since a critical multiset is a gathering of numbers whose sum is particularly large, we can bound the sum $h_{ji_1}\odot\tilde{c}_{(i_1,l)}+\cdots+h_{ji_t}\odot\tilde{c}_{(i_t,l)}$ below by $(t-1)p$. Thanks to Corollary 3.5, similar statements hold for any multisubset of $\{\gamma_1,\ldots,\gamma_t\}$. The coefficient $a\in\mathbb{F}_p^*$ makes sure that multiples of $\tilde{\mathbf{c}}$ are taken into consideration. Finally, the parity condition serves as a counterpart to the parity-check matrix H.

We will see later that the bounds from Theorem 3.11 are sufficient descriptions of the pseudocodewords for $p=2$ and $p=3$. An interesting aspect of this fact is that for these cases the attributes $\Theta_j({}^a\mathcal{M})$, $a\in\mathbb{F}_p^*$, are powerful enough to determine if $\mathcal{M}$ is a pseudocodeword, given that certain sums of the entries of $\mathcal{M}$ do not exceed this quantity. For larger primes p, the conditions considered above may only provide a necessary condition that pseudocodewords of codes over $\mathbb{F}_p$ must satisfy; determining a set of sufficient conditions remains a topic of further study. This will be demonstrated in Example 5.1.

Next, we relate the bounds given in Theorem 3.11 to the fundamental cone of a parity-check matrix. Before doing so, we recall its definition.

Definition 3.14: The fundamental cone of $H\in\mathbb{F}_p^{n\times r}$, denoted $\mathcal{K}_p(H)$, is the smallest cone in $\mathbb{R}^{(p-1)n}$ that contains all pseudocodewords of $C(H)$.

The fundamental cone $\mathcal{K}_2(H)$ of a binary code $C(H)$ has been studied extensively in the literature (see, for instance, [17], [18], [19]). The ternary case has been investigated by Skachek [22].

Notice that the bounds given in Theorem 3.11 may be used to define a cone in $\mathbb{R}^{(p-1)n}$ as follows. Given $H\in\mathbb{F}_p^{r\times n}$, let

$$\begin{aligned}
&K_p(H) \coloneqq \\
&\left\{ \mathbf{m} :\ \begin{array}{l} \Theta_j({}^a\mathcal{M}(\mathbf{m})) \ge \mathbf{1}\,\mathrm{Col}_i\,\mathcal{M}(\mathbf{m}) \text{ and} \\ \Theta_j({}^a\mathcal{M}(\mathbf{m})) \ge \sum_{l=1}^t m_{\left(\gamma_l\odot a^{-1}\odot h_{ji_l}^{-1}-1\right)n+i_l} \\ \forall 1\le j\le r, i, i_1,\ldots,i_t\in \mathrm{supp}\left(\mathrm{Row}_j(H)\right), \\ a\in\mathbb{F}_p^*, \{\gamma_1,\ldots,\gamma_t\}\in\Gamma_p^* \end{array} \right\} \\
&\subseteq\ \mathbb{R}_{\ge 0}^{(p-1)n}.
\end{aligned}$$

The cone defined above coincides with the fundamental cone for $p=2$ and $p=3$. We shall restate this fact in the following proposition.

Proposition 3.15: The cone $K_p(H)$ is the fundamental cone for $p=2$ and $p=3$. In other words, $K_2(H)=\mathcal{K}_2(H)$ and $K_3(H)=\mathcal{K}_3(H)$.

Copyright (c) 2014 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TIT.2014.2331677

Proof Since 1 is the only nonzero element in $\mathbb{F}_2$, we have

$$\Theta_j(\mathcal{M}(\mathbf{m})) = \frac{1}{2}\,\mathrm{Row}_j(H)\mathbf{m}^T.$$

In addition, as $\mathbb{F}_2$ contains no critical multisets, one may simplify $K_2(H)$ to

$$K_2(H) = \left\{ \mathbf{m} \in \mathbb{R}^n_{\geq 0} : \begin{array}{l} \mathrm{Row}_j(H)\mathbf{m}^T \geq 2m_i \\ \forall 1 \leq j \leq r, i \in \mathrm{supp}\left(\mathrm{Row}_j(H)\right) \end{array} \right\}.$$

As a result, $K_2(H) = \mathcal{K}_2(H)$ according to [18].

Now, $a = a^{-1}$ for $a \in \mathbb{F}_3^*$, and the only critical multiset of $\mathbb{F}_3$ is $\{2, 2\}$. So,

$$K_3(H) = \left\{ \mathbf{m} \in \mathbb{R}^{2n}_{\geq 0} : \begin{array}{l} \Theta_j({}^a\mathcal{M}(\mathbf{m})) \geq m_i + m_{n+i} \text{ and} \\ \Theta_j({}^a\mathcal{M}(\mathbf{m})) \geq m_{(2\odot a^{-1}\odot h_{ji_1}-1)n+i_1} \\ \qquad\qquad + m_{(2\odot a^{-1}\odot h_{ji_2}-1)n+i_2} \\ \forall 1 \leq j \leq r, \\ i, i_1, i_2 \in \mathrm{supp}(\mathrm{Row}_j(H)), a \in \mathbb{F}_3^* \end{array} \right\}.$$

It follows that this cone coincides with the fundamental cone of $C(H)$ [22], meaning $K_3(H) = \mathcal{K}_3(H)$. ∎

The next result follows immediately from the definition of $K_p(H)$ and Theorem 3.11.

Proposition 3.16: Let $H \in \mathbb{F}_p^{r\times n}$ and $\mathbf{m} \in \mathbb{N}^{(p-1)n}$. If $\mathbf{m}$ is a pseudocodeword of $C(H)$, then $\mathbf{m} \in K_p(H)$ and

$$H\mathcal{M}(\mathbf{m})^T \begin{bmatrix} 1 \\ 2 \\ \vdots \\ p-1 \end{bmatrix} \mod p = \mathbf{0};$$

that is,

$$\mathcal{PC}(H) \subseteq \left\{ \mathbf{m} \in K_p(H) : H\mathcal{M}(\mathbf{m})^T \begin{bmatrix} 1 \\ 2 \\ \vdots \\ p-1 \end{bmatrix} \mod p = \mathbf{0} \right\}.$$

Remark 3.17: If $p = 2$ or $p = 3$, then the converse holds [17], [22, Theorem 4.7]; that is,

$$\mathcal{PC}(H) = \left\{ \mathbf{m} \in K_p(H) : H\mathcal{M}(\mathbf{m})^T \begin{bmatrix} 1 \\ 2 \\ \vdots \\ p-1 \end{bmatrix} \mod p = \mathbf{0} \right\}$$

if $p = 2, 3$. Hence, Proposition 3.16 provides a characterization of binary and ternary pseudocodewords. For all primes p, we have $\mathcal{K}_p(H) \subseteq K_p(H)$.

B. Irreducible and minimal pseudocodewords

We are now equipped to investigate *irreducible* and *minimal* pseudocodewords. As we will demonstrate, these pseudocodewords are most likely to cause decoding failure for LP and iterative decoding algorithms on the p-ary symmetric channel. Due to the symmetry conditions on the channel, the probability of codeword error is independent of the codeword transmitted; see [8, Example 5.1]. Hence, we may assume the all-zero codeword is transmitted. Then, low pseudoweight pseudocodewords play the role in LP and iterative decoding algorithms that the low weight codewords do in maximum likelihood decoding [26], [28]. To make this precise, we need a few definitions.

Definition 3.18:

1) A nonzero pseudocodeword is said to be *irreducible* provided it cannot be written as a sum of two or more nonzero pseudocodewords. We denote by $Irr(H)$ the set of all irreducible pseudocodewords of $C(H)$.
2) A pseudocodeword $\mathbf{v}$ is called *minimal* provided $\{\lambda\mathbf{v} : \lambda \in \mathbb{R}, \lambda \geq 0\}$ is an edge of the fundamental cone $\mathcal{K}_P(H)$.

It follows from the definition that any pseudocodeword can be written as a sum of irreducible pseudocodewords. Therefore, characterizing the irreducible pseudocodewords is sufficient to describe the set of all pseudocodewords. From a mathematical point of view, the sets of irreducible pseudocodewords and minimal pseudocodewords are important, because irreducible pseudocodewords are a $\mathbb{Z}$-basis for $\mathcal{PC}(H)$ whereas minimal pseudocodewords form an $\mathbb{R}$-basis for $\mathcal{K}_p(H)$. Here, the term basis is used in the conic sense, meaning that the set of irreducible codewords (resp., minimal pseudocodewords) generates the set $\mathcal{PC}(H)$ (resp., $\mathcal{K}_p(H)$) via conical combinations $\sum a_i v_i$ with $a_i \in \mathbb{Z}$ (resp., $\mathbb{R}$) and $a_i \geq 0$.

From a decoding point of view, irreducible pseudocodewords and minimal pseudocodewords are important. Indeed, as we demonstrate below, the pseudoweight of a pseudocodeword on the p-ary symmetric channel is bounded below by the minimum of the pseudoweights of its irreducible pseudocodeword components. We recall the definition for the pseudoweight of a nonbinary pseudocodeword on the p-ary symmetric channel as follows.

Definition 3.19: [16, Definition 3.1] Let $H \in \mathbb{F}_p^{r\times n}$ and let $\mathcal{M}$ be a pseudocodeword of $C(H)$ in matrix form. Let e be the smallest number with the property that if $m_{i_1}(b_1), \ldots, m_{i_e}(b_e)$ are the e largest components

Copyright (c) 2014 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TIT.2014.2331677

from distinct columns of $\mathcal{M}$ then

$$\sum_{e'=1}^{e} m_{i_{e'}}(b_{e'}) \geq \sum_{i \notin \{i_1, \ldots i_e\}} \sum_{b=1}^{p-1} m_i(b).$$

The pseudoweight of $\mathcal{M}$ on the p-ary symmetric channel is given by

$$w_p(\mathcal{M}) := \begin{cases} 2e & \text{if } \sum_{e'=1}^{e} m_{i_{e'}}(b_{e'}) \\ & \quad = \sum_{i \notin \{i_1, \ldots i_e\}} \sum_{b=1}^{p-1} m_i(b), \\ 2e-1 & \text{if } \sum_{e'=1}^{e} m_{i_{e'}}(b_{e'}) \\ & \quad > \sum_{i \notin \{i_1, \ldots i_e\}} \sum_{b=1}^{p-1} m_i(b). \end{cases}$$

Proposition 3.20: Let $\mathcal{M}_1, \mathcal{M}_2$ be pseudocodeword matrices of $C(H)$ where $H \in \mathbb{F}_p^{r \times n}$. If $\mathcal{M}_3 = \mathcal{M}_1 + \mathcal{M}_2$, then $w_p(\mathcal{M}_3) \geq \min\{w_p(\mathcal{M}_1), w_p(\mathcal{M}_2)\}$. Hence, for any pseudocodeword matrix $\mathcal{M}$ of $C(H)$,

$$w_p(\mathcal{M}) \geq \min\left\{w_p(\mathcal{M}_I) : \mathcal{M}_I \in Irr(H)\right\}.$$

Proof We distinguish the components of $\mathcal{M}_1, \mathcal{M}_2$, and $\mathcal{M}_3$ using $m_i^1(b), m_i^2(b)$, and $m_i^3(b)$ respectively, where $1 \leq i \leq n$ and $1 \leq b \leq p-1$. Now, if

$$\sum_{e'=1}^{e} m_{i_{e'}}^3(b_{e'}) > \sum_{i \neq i_1, \ldots i_e} \sum_{b=1}^{p-1} m_i^3(b),$$

then either

$$\sum_{e'=1}^{e} m_{i_{e'}}^1(b_{e'}) > \sum_{i \neq i_1, \ldots i_e} \sum_{b=1}^{p-1} m_i^1(b)$$

or

$$\sum_{e'=1}^{e} m_{i_{e'}}^2(b_{e'}) > \sum_{i \neq i_1, \ldots i_e} \sum_{b=1}^{p-1} m_i^2(b).$$

On the other hand, if

$$\sum_{e'=1}^{e} m_{i_{e'}}^3(b_{e'}) = \sum_{i \neq i_1, \ldots i_e} \sum_{b=1}^{p-1} m_i^3(b),$$

then either

$$\sum_{e'=1}^{e} m_{i_{e'}}^1(b_{e'}) \geq \sum_{i \neq i_1, \ldots i_e} \sum_{b=1}^{p-1} m_i^1(b)$$

or

$$\sum_{e'=1}^{e} m_{i_{e'}}^2(b_{e'}) \geq \sum_{i \neq i_1, \ldots i_e} \sum_{b=1}^{p-1} m_i^2(b).$$

In both cases it readily follows that

$$w_p(\mathcal{M}_3) \geq \min\{w_p(\mathcal{M}_1), w_p(\mathcal{M}_1)\}.$$

∎

It follows from the previous proposition that pseudocodewords with low pseudoweight must be irreducible. Hence, irreducible pseudocodewords are especially problematic for LP and iterative decoders as they are most likely to be confused with the all-zero word due to their lower pseudoweights.

We close this section with an observation relating the sets of irreducible and minimal pseudocodewords of a p-ary parity-check code.

Proposition 3.21: Let $H \in \mathbb{F}_p^{r \times n}$. Then the set of irreducible pseudocodewords $Irr(H)$ contains a multiple of each minimal pseudocodeword of $C(H)$.

Proof Let $\mathbf{m}$ be a pseudocodeword and suppose that $\mathbf{m} \notin Irr(H)$. Then certainly $\mathbf{m} = \mathbf{m}_1 + \mathbf{m}_2$ for some $\mathbf{m}_1, \mathbf{m}_2 \in \mathcal{PC}(H)$. From this, it follows that

$$\{\lambda \mathbf{m} | \lambda \in \mathbb{R}_+\}$$

is not an extreme ray of $\mathcal{K}_3(H)$. Hence, $\mathbf{m}$ is not a minimal pseudocodeword. ∎

From the previous proposition, we see that each minimal pseudocodeword gives rise to an irreducible pseudocodeword. However, it is not necessary that all irreducible pseudocodewords arise in this way. Example 5.2 in Section V will demonstrate this presumption.

In the next section, we will develop tools which allow us to find the irreducible pseudocodewords of codes over $\mathbb{F}_3$, just as in the binary case [19].

IV. Ternary pseudocodewords

In this section, we focus on pseudocodewords of ternary codes over the ternary symmetric channel. Recall from the previous section that for $H \in \mathbb{F}_3^{r \times n}$ and $\mathbf{m} \in \mathbb{N}^{2n}$, the following are equivalent:

1) $\mathbf{m}$ is a pseudocodeword of $C(H)$.
2) $\mathbf{m} \in \mathcal{K}_3(H)$ and

$$H\mathcal{M}(\mathbf{m})^T \begin{bmatrix} 1 \\ 2 \end{bmatrix} \mod 3 = \mathbf{0}.$$

While this result characterizes the points within the fundamental cone that are pseudocodewords, it is convenient to have a cone whose integer points are in a one-to-one correspondence with the pseudocodewords of $C(H)$. This is due to the fact that there are a number of algorithms and computational tools available for computing integer points in rational cones. The application of these tools in the binary case is detailed in [19]. With this in mind, we define the lifted fundamental cone of a ternary code.

Copyright (c) 2014 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TIT.2014.2331677

Definition 4.1: Given $H \in \mathbb{F}_3^{r\times n}$, the lifted fundamental cone of $C(H)$ is

$$\hat{\mathcal{K}}_3(H) \coloneqq \left\{ (\mathbf{m},\mathbf{a}) \in \mathbb{R}^{2n+r} : \begin{array}{l} \mathbf{m} \in \mathcal{K}_3(H), \\ H\mathcal{M}(\mathbf{m})^T \begin{bmatrix} 1 \\ 2 \end{bmatrix} = 3\mathbf{a}^T \end{array} \right\}.$$

Now, the lifted fundamental cone and the fundamental cone can be related via the projection

$$\begin{array}{rccc} \pi: & \mathbb{R}^{2n+r} & \to & \mathbb{R}^{2n} \\ & (\mathbf{m},\mathbf{a}) & \mapsto & \mathbf{m}. \end{array} \tag{10}$$

The relationship between the lifted cone $\hat{\mathcal{K}}_3(H)$, the fundamental cone $\mathcal{K}_3(H)$, and the pseudocodewords of $C(H)$ is made precise in the following proposition.

Proposition 4.2: Let $H \in \mathbb{F}_3^{r\times n}$. The projection $\pi|_{\hat{\mathcal{K}}_3(H)}$ is one-to-one and

$$\pi\left(\hat{\mathcal{K}}_3(H)\right) = \mathcal{K}_3(H).$$

Furthermore,

$$\pi\left(\hat{\mathcal{K}}_3(H) \cap \mathbb{Z}^{n+r}\right) = \mathcal{PC}(H).$$

In other words, $\hat{\mathcal{K}}_3(H)$ is a cone in $\mathbb{R}^{2n+r}$ whose projection is $\mathcal{K}_3(H)$, and its integer points correspond precisely to the pseudocodewords of $C(H)$.

Proof Suppose that $\pi(\mathbf{m},\mathbf{a}) = \pi(\mathbf{m}',\mathbf{a}')$ where $(\mathbf{m},\mathbf{a}),(\mathbf{m}',\mathbf{a}') \in \hat{\mathcal{K}}_3(H)$. Then $\mathbf{m} = \mathbf{m}'$ and

$$3\mathbf{a}^T = H\mathcal{M}(\mathbf{m})^T \begin{bmatrix} 1 \\ 2 \end{bmatrix} = H\mathcal{M}(\mathbf{m}')^T \begin{bmatrix} 1 \\ 2 \end{bmatrix} = 3\mathbf{a}'^T.$$

We can then conclude that $(\mathbf{m},\mathbf{a}) = (\mathbf{m}',\mathbf{a}')$. Hence, $\pi|_{\hat{\mathcal{K}}_3(H)}$ is injective.

Now,

$$\begin{aligned} &\pi\left(\hat{\mathcal{K}}_3(H)\right) \\ &= \left\{ \mathbf{m} \in \mathbb{R}^{2n} : \begin{array}{l} \mathbf{m} \in \mathcal{K}_3(H) \text{ and} \\ H\mathcal{M}(\mathbf{m})^T \begin{bmatrix} 1 \\ 2 \end{bmatrix} = 3\mathbf{a}^T \\ \text{for some } \mathbf{a} \in \mathbb{R}^r \end{array} \right\} \\ &= \mathcal{K}_3(H). \end{aligned}$$

Lastly, let $(\mathbf{m},\mathbf{a})$ be an integer point in $\hat{\mathcal{K}}_3(H)$. Then, $\mathbf{m} = \pi(\mathbf{m},\mathbf{a}) \in \mathcal{K}_3(H)$ and $H\mathcal{M}(\mathbf{m})^T \begin{bmatrix} 1 \\ 2 \end{bmatrix} = 3\mathbf{a}^T$, implying that $H\mathcal{M}(\mathbf{m})^T \begin{bmatrix} 1 \\ 2 \end{bmatrix} \mod 3 = \mathbf{0}$. By Remark 3.17, $\pi(\mathbf{m},\mathbf{a}) = \mathbf{m}$ is a pseudocodeword of $C(H)$. On the other hand, let $\mathbf{m} \in \mathcal{PC}(H)$. Then $\mathbf{m}$ is an integer vector in $\mathcal{K}_3(H)$ such that

$$H\mathcal{M}(\mathbf{m})^T \begin{bmatrix} 1 \\ 2 \end{bmatrix} \mod 3 = \mathbf{0}.$$

Since $\pi\left(\hat{\mathcal{K}}_3(H)\right) = \mathcal{K}_3(H)$, $(\mathbf{m},\mathbf{a}) \in \hat{\mathcal{K}}_3(H)$ for some $\mathbf{a} \in \mathbb{R}^r$. The fact that

$$H\mathcal{M}(\mathbf{m})^T \begin{bmatrix} 1 \\ 2 \end{bmatrix} \mod 3 = \mathbf{0}$$

implies $\mathbf{a} \in \mathbb{Z}^r$. We conclude that $\pi\left(\hat{\mathcal{K}}_3(H) \cap \mathbb{Z}^{n+r}\right) = \mathcal{PC}(H)$. ∎

Next, we will see that the lifted fundamental cone allows us to find the irreducible pseudocodewords via Proposition 4.2. We review here terminology that will be helpful in demonstrating this. The lifted fundamental cone is certainly a *rational cone*; a rational cone K is the solution space of a system of finitely many linear inequalities with integer coefficients such that $\lambda\mathbf{v} \in K$ for all $\mathbf{v} \in K$ and $\lambda \geq 0$. A rational cone is *pointed* provided it has a vertex at the origin. The set of integer vectors in a rational cone whose vertex is at the origin forms an additive semigroup. The minimal set of generators $\mathcal{B}$ of this semigroup is called the *Hilbert basis* of the cone. More precisely, given a pointed rational cone $K \subseteq \mathbb{R}^n$, the Hilbert basis of K is the minimal set of vectors $\{\mathbf{b}_1,\ldots,\mathbf{b}_t\}$ with the property that

$$\{\lambda_1\mathbf{b}_1 + \cdots + \lambda_t\mathbf{b}_t : \lambda_1,\ldots,\lambda_t \in \mathbb{N}\} = K \cap \mathbb{Z}^n.$$

The following proposition relates the Hilbert basis of the lifted fundamental cone $\hat{\mathcal{K}}_3(H)$ to the irreducible pseudocodewords of $C(H)$.

Proposition 4.3: Let $H \in \mathbb{F}_3^{r\times n}$. The set of irreducible pseudocodewords of $C(H)$ is

$$Irr(H) = \pi(\mathcal{B})$$

where $\mathcal{B}$ is the Hilbert basis of $\hat{\mathcal{K}}_3(H)$; that is, the set of irreducible pseudocodewords of $C(H)$ can be found as a projection of the Hilbert basis of the lifted fundamental cone of $C(H)$.

Proof Let $\mathcal{B} \coloneqq \{\mathbf{b}_1,\ldots,\mathbf{b}_t\}$ be the Hilbert basis of $\hat{\mathcal{K}}_3(H)$.

Let $\mathbf{p} \in Irr(H)$ be an irreducible pseudocodeword of $C(H)$. By Proposition 4.2, $\mathbf{p} = \pi(\mathbf{y})$ for some $\mathbf{y} \in \hat{\mathcal{K}}_3(H) \cap \mathbb{Z}^{n+r}$. Since $\mathcal{B}$ is a Hilbert basis for $\hat{\mathcal{K}}_3(H)$, $\mathbf{y} = \sum_{i=1}^t \lambda_i\mathbf{b}_i$ for some $\lambda_i \in \mathbb{Z}$ with $\lambda_i \geq 0$. Clearly,

$$\pi(\mathbf{y}) = \sum_{i=1}^t \lambda_i \pi(\mathbf{b}_i).$$

According to Proposition 4.2, each $\pi(\mathbf{b}_i)$ is a pseudocodeword. Being irreducible, $\mathbf{p}$ cannot be written as a sum of two or more nonzero pseudocodewords. Thus, $\lambda_i = 1$ for some $i \in \{1,\ldots,t\}$ and $\lambda_j = 0$ for all $j \neq i$. Therefore, $\mathbf{p} = \pi(\mathbf{b}_i)$ and $Irr(H) \subseteq \pi(\mathcal{B})$.

Copyright (c) 2014 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TIT.2014.2331677

Now consider $\pi(\mathbf{b})$ where $\mathbf{b} \in \mathcal{B}$. Since $\mathbf{b} \in \hat{\mathcal{K}}_3(H) \cap \mathbb{Z}^{n+r}$, $\pi(\mathbf{b})$ is a pseudocodeword by Proposition 4.2. Suppose $\pi(\mathbf{b}) = \mathbf{p}_1 + \mathbf{p}_2$ for some nonzero pseudocodewords $\mathbf{p}_1$ and $\mathbf{p}_2$ of $C(H)$. By Proposition 4.2, $\mathbf{p}_1 = \pi(\mathbf{p}_1, \mathbf{a}_1)$ and $\mathbf{p}_2 = \pi(\mathbf{p}_2, \mathbf{a}_2)$ for some $(\mathbf{p}_1, \mathbf{a}_1), (\mathbf{p}_2, \mathbf{a}_2) \in \hat{\mathcal{K}}_3(H)$. It then follows that

$$\mathbf{b} = (\mathbf{p}_1, \mathbf{a}_1) + (\mathbf{p}_2, \mathbf{a}_2),$$

contradicting the minimality of $\mathcal{B}$. Therefore, $\pi(\mathbf{b})$ is irreducible, and $\pi(\mathcal{B}) \subseteq Irr(H)$. ∎

Definition 4.4: Given $H \in \mathbb{F}_3^{r\times n}$, the t-value of the Tanner graph of H, denoted t, is defined to be the maximum value that a coordinate of an irreducible pseudocodeword of $C(H)$ can have; that is,

$$t \coloneqq \max\{m_i : \mathbf{m} \in Irr(H)\}.$$

According to [15, Theorem 3.5], the t-value of a Tanner graph corresponding to a binary parity-check code is finite. Next, we obtain an analogous result for ternary parity-check codes as a corollary to Proposition 4.3.

Corollary 4.5: Given $H \in \mathbb{F}_3^{r\times n}$, the t-value of the Tanner graph of H is finite.

Proof Let $H \in \mathbb{F}_3^{r\times n}$. According to [4], the lifted fundamental cone $\hat{\mathcal{K}}_3(H)$ has a unique Hilbert basis $\mathcal{B}$. Applying Proposition 4.3, we see that the set of irreducible pseudocodewords of $C(H)$ is $Irr(H) = \pi(\mathcal{B})$. The result follows from the fact that the Hilbert basis $\mathcal{B}$ is finite [13]. ∎

V. Examples

Example 5.1 below demonstrates bounds from Theorem 3.11 for a code over $\mathbb{F}_5$. As we will see, there are words which are not pseudocodewords that satisfy the bounds, indicating that the cone $K_p(H)$ is not tight in general.

In Example 5.2, we find irreducible and minimal pseudocodewords of a ternary code with two different choices for the parity-check matrix. We will see in this example that the representation of a code greatly impacts the set of pseudocodewords.

Example 5.1: Consider a code C(H) over $\mathbb{F}_5$ given by a parity-check matrix

$$H = \begin{bmatrix} 1 & 1 & 2 & 4 \\ 0 & 3 & 3 & 0 \end{bmatrix} \in \mathbb{F}_5^{2\times 4}.$$

We then have

$$\begin{aligned}\Theta_1(\mathcal{M}) &= \frac{1}{5}\sum_{b=1}^{4}\Big(b \odot \operatorname{Row}_1(H)\Big)\operatorname{Row}_b(\mathcal{M})^T \\ &= \frac{1}{5}\Big(\begin{pmatrix}1&1&2&4\end{pmatrix}\operatorname{Row}_1(\mathcal{M})^T \\ &\quad + \begin{pmatrix}2&2&4&3\end{pmatrix}\operatorname{Row}_2(\mathcal{M})^T \\ &\quad + \begin{pmatrix}3&3&1&2\end{pmatrix}\operatorname{Row}_3(\mathcal{M})^T \\ &\quad + \begin{pmatrix}4&4&3&1\end{pmatrix}\operatorname{Row}_4(\mathcal{M})^T\Big)\end{aligned}$$

and

$$\begin{aligned}\Theta_2(\mathcal{M}) &= \frac{1}{5}\sum_{b=1}^{4}\Big(b \odot \operatorname{Row}_2(H)\Big)\operatorname{Row}_b(\mathcal{M})^T \\ &= \frac{1}{5}\Big(\begin{pmatrix}0&3&3&0\end{pmatrix}\operatorname{Row}_1(\mathcal{M})^T \\ &\quad + \begin{pmatrix}0&1&1&0\end{pmatrix}\operatorname{Row}_2(\mathcal{M})^T \\ &\quad + \begin{pmatrix}0&4&4&0\end{pmatrix}\operatorname{Row}_3(\mathcal{M})^T \\ &\quad + \begin{pmatrix}0&2&2&0\end{pmatrix}\operatorname{Row}_4(\mathcal{M})^T\Big).\end{aligned}$$

The column sum bounds for the pseudocodewords of $C(H)$ are given by

$$\begin{aligned}\Theta_1({}^a\mathcal{M}) &\geq m_1(1)+m_1(2)+m_1(3)+m_1(4),\\ \Theta_1({}^a\mathcal{M}) &\geq m_2(1)+m_2(2)+m_2(3)+m_2(4),\\ \Theta_1({}^a\mathcal{M}) &\geq m_3(1)+m_3(2)+m_3(3)+m_3(4),\\ \Theta_1({}^a\mathcal{M}) &\geq m_4(1)+m_4(2)+m_4(3)+m_4(4),\\ \Theta_2({}^a\mathcal{M}) &\geq m_2(1)+m_2(2)+m_2(3)+m_2(4),\\ \Theta_2({}^a\mathcal{M}) &\geq m_3(1)+m_3(2)+m_3(3)+m_3(4),\end{aligned}$$

for all $a \in \{1,2,3,4\}$. Now, recall that critical multisets of $\mathbb{F}_5$ are

$$\begin{aligned}\Gamma_5 = \{&\{2,4\},\{3,3\},\{3,4\},\{4,4\},\\ &\{3,4,4\},\{4,4,4\},\{4,4,4,4\}\}.\end{aligned}$$

We will list the critical multiset bounds that correspond to the multisets $\{2,4\}$ and $\{4,4,4,4\}$. The ones resulting

Copyright (c) 2014 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TIT.2014.2331677

from $\{2, 4\}$ are

$$\begin{aligned}
\Theta_1({}^a\mathcal{M}) &\geq m_1(a^{-1} \odot 2) + m_2(a^{-1} \odot 4),\\
\Theta_1({}^a\mathcal{M}) &\geq m_1(a^{-1} \odot 4) + m_2(a^{-1} \odot 2),\\
\Theta_1({}^a\mathcal{M}) &\geq m_1(a^{-1} \odot 2) + m_3(a^{-1} \odot 2),\\
\Theta_1({}^a\mathcal{M}) &\geq m_1(a^{-1} \odot 4) + m_3(a^{-1} \odot 1),\\
\Theta_1({}^a\mathcal{M}) &\geq m_1(a^{-1} \odot 2) + m_4(a^{-1} \odot 1),\\
\Theta_1({}^a\mathcal{M}) &\geq m_1(a^{-1} \odot 4) + m_4(a^{-1} \odot 3),\\
\Theta_1({}^a\mathcal{M}) &\geq m_2(a^{-1} \odot 2) + m_3(a^{-1} \odot 2),\\
\Theta_1({}^a\mathcal{M}) &\geq m_2(a^{-1} \odot 4) + m_3(a^{-1} \odot 1),\\
\Theta_1({}^a\mathcal{M}) &\geq m_2(a^{-1} \odot 2) + m_4(a^{-1} \odot 1),\\
\Theta_1({}^a\mathcal{M}) &\geq m_2(a^{-1} \odot 4) + m_4(a^{-1} \odot 3),\\
\Theta_1({}^a\mathcal{M}) &\geq m_3(a^{-1} \odot 1) + m_4(a^{-1} \odot 1),\\
\Theta_1({}^a\mathcal{M}) &\geq m_3(a^{-1} \odot 2) + m_4(a^{-1} \odot 3),
\end{aligned}$$

and

$$\begin{aligned}
\Theta_2({}^a\mathcal{M}) &\geq m_2(a^{-1} \odot 4) + m_3(a^{-1} \odot 3),\\
\Theta_2({}^a\mathcal{M}) &\geq m_2(a^{-1} \odot 3) + m_3(a^{-1} \odot 4)
\end{aligned}$$

where $a \in \{1, 2, 3, 4\}$. The critical multiset bounds from $\{4, 4, 4, 4\}$ are

$$\begin{aligned}
\Theta_1({}^a\mathcal{M}) \geq\ & m_1(a^{-1} \odot 4) + m_2(a^{-1} \odot 4)\\
&+ m_3(a^{-1} \odot 2) + m_4(a^{-1} \odot 1)
\end{aligned}$$

where $a \in \{1, 2, 3, 4\}$.

Consider now an integer matrix

$$\mathcal{M}' = \begin{bmatrix} 5 & 0 & 0 & 0\\ 0 & 0 & 0 & 5\\ 0 & 0 & 0 & 5\\ 5 & 0 & 0 & 0 \end{bmatrix}.$$

It is easily shown that $\Theta_1({}^a\mathcal{M}') = 10$ and $\Theta_2({}^a\mathcal{M}') = 0$ for all a, and $\mathcal{M}'$ satisfies all bounds given in Theorem 3.11. However, there does not exist a codeword on a graph cover of H that corresponds to $\mathcal{M}'$ since no combination on the possible values for the first and last symbol node ($\{1, 4\}$ and $\{2, 3\}$, respectively) can be made to satisfy the first parity-check.

Example 5.2: In this example, we consider a [4,2] ternary linear code with two different choices of parity-check matrix. Let

$$H_1 = \begin{bmatrix} 1 & 2 & 2 & 1\\ 2 & 0 & 1 & 2 \end{bmatrix}$$

and

$$H_2 = \begin{bmatrix} 0 & 2 & 0 & 0\\ 2 & 0 & 1 & 2 \end{bmatrix}.$$

Note that first row of H_2 is the sum of the two rows of H_1. Hence,

$$C(H_1) = C(H_2).$$

Using 4ti2 [14] and Proposition 4.3, we find the irreducible pseudocodewords of $C(H_1)$ and $C(H_2)$.

The irreducible pseudocodewords of $C(H_1)$ are listed below:

$$\begin{array}{ll}
(0,0,0,0,0,0,1,1), & (0,0,0,0,1,0,1,0),\\
(0,0,0,1,1,0,0,0), & (0,0,1,0,1,0,0,1),\\
(0,0,1,1,0,0,0,0), & (1,0,0,0,0,0,0,1),\\
(1,0,0,1,0,0,1,0), & (1,0,1,0,0,0,0,0),\\
(0,0,0,1,1,3,1,1), & (0,0,0,1,2,3,1,0),\\
(0,0,1,0,1,3,0,1), & (0,0,1,1,0,3,1,1),\\
(0,0,1,1,1,3,1,0), & (0,1,0,0,0,1,1,1),\\
(0,1,0,0,1,1,1,0), & (0,1,0,1,1,1,0,0),\\
(0,1,1,0,1,1,0,1), & (0,1,1,1,0,1,0,0),\\
(0,3,0,0,1,0,2,1), & (0,3,0,1,1,0,1,1),\\
(0,3,1,0,1,0,1,2), & (0,3,1,0,2,0,1,1),\\
(0,3,1,1,0,0,1,1), & (0,3,1,1,1,0,1,0),\\
(0,3,1,1,2,0,0,1), & (0,3,1,2,1,0,0,0),\\
(0,3,2,0,2,0,0,2), & (0,3,2,1,1,0,0,1),\\
(1,0,0,0,0,3,1,2), & (1,0,0,0,1,3,1,1),\\
(1,0,0,1,0,3,2,1), & (1,0,0,1,1,3,0,1),\\
(1,0,0,1,1,3,2,0), & (1,0,0,2,1,3,1,0),\\
(1,0,1,0,0,3,1,1), & (1,0,1,0,1,3,1,0),\\
(1,0,1,1,0,3,0,1), & (1,0,1,1,1,3,0,0),\\
(1,0,1,2,0,3,1,0), & (1,0,2,1,0,3,0,0),\\
(1,1,0,0,0,1,0,1), & (1,1,0,1,0,1,1,0),\\
(1,1,1,0,0,1,0,0), & (1,3,0,0,1,0,1,1),\\
(1,3,0,1,0,0,1,0), & (1,3,0,1,1,0,0,1),\\
(1,3,1,0,0,0,1,1), & (1,3,1,0,1,0,0,2),\\
(1,3,1,0,1,0,1,0), & (1,3,1,1,0,0,0,1),\\
(1,3,1,1,1,0,0,0), & (1,3,2,0,1,0,0,1),\\
(2,0,0,1,0,3,1,1), & (2,0,0,2,0,3,2,0),\\
(2,0,1,1,0,3,1,0), & (2,3,1,0,0,0,0,1).
\end{array}$$

On the other hand, the irreducible pseudocodewords of $C(H_2)$ are the first eight pseudocodewords listed above, which correspond precisely to the codewords of $C(H_1) = C(H_2)$. One may note that the Tanner graph of H_2 is cycle-free. Hence, this coincides with the theoretical result that a code with a cycle-free Tanner graph representation has no non-codeword pseudocodewords.

The minimal pseudocodewords of $C(H_1)$ consist of all the pseudocodewords listed above except $(0, 1, 1, 0, 1, 1, 0, 1)$ and $(1, 1, 0, 1, 0, 1, 1, 0)$. The minimal pseudocodewords of $C(H_2)$ are, once again, simply the eight codewords of $C(H_1) = C(H_2)$.

VI. Conclusion

In this paper, we consider pseudocodewords of parity-check codes over $\mathbb{F}_p$ where p is prime. Inequalities that define a cone containing all pseudocodewords are given. In the cases $p = 2$ and 3, this cone is precisely the fundamental cone. For larger primes p, a precise

Copyright (c) 2014 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TIT.2014.2331677

system of inequalities defining the fundamental cone of a p-ary code remains a topic of investigation; this paper contains progress toward that goal. For ternary codes, Hilbert bases are used to determine the irreducible pseudocodewords; this characterization provides insight into the minimal pseudocodewords as well. This method enables the study of the choice of code representation for parity-check codes over prime alphabets.

ACKNOWLEDGMENT

The authors wish to thank the reviewers for their helpful comments and suggestions.

REFERENCES

[1] N. Axvig, D. Dreher, K. Morrison, E. Psota, L. C. Perez, J. L. Walker, Analysis of connections between pseudocodewords, IEEE Trans. Inform. Theory **55** (2009), no. 9, pp. 4099–4107.

[2] D. Burshtein and I. Goldenberg, Improved linear programming decoding of LDPC codes and bounds on the minimum and fractional distance, IEEE Trans. Inform. Theory **57** (2011), no. 11, pp. 7386–7402.

[3] M. Chertkov and M. Stepanov, Pseudo-codeword landscape, Proc. IEEE Int. Symp. Inf. Theory, June 2007, pp. 1546–1550, Nice, France.

[4] J. G. van der Corput, Über systeme von linear-homogenen gleichungen und ungleichungen, Proc. Koninklijke Akademie van Wetenschappen te Amsterdam **34**, 368–371 (1931).

[5] M. C. Davey and D. J. C. MacKay, Low density parity-check codes over $GF(q)$, IEEE Communications Letters **2** (1998), no. 6, 159–166.

[6] J. Feldman, Decoding error-correcting codes via linear programming, PhD thesis, Massachusetts Institute of Technology, 2003.

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

[8] M. Flanagan, V. Skachek, E. Byrne, and M. Greferath, Linear-programming decoding of nonbinary linear codes, IEEE Trans. Inform. Theory **55** (2009), no. 9, 4134–4154.

[9] G.D. Forney, Jr., and G. Ungerboeck, Modulation and coding for linear Gaussian channels, IEEE Trans. Inform. Theory **44** (1998), no. 6, pp. 2384–2415.

[10] K. Fukuda, CDD and CDD+ Homepage 2008 [Online]. Available: http://www.ifor.math.ethz.ch/~fukuda/cdd_home/cdd.html.

[11] K. Fukuda and A. Prodon, Double description method revisited, Lecture Notes in Comput. Sci. **1120**(1996), 91–111.

[12] D. Goldin and D. Burshtein, Iterative linear programming decoding of nonbinary LDPC codes with linear complexity **59** (2013), no. 1, pp. 282–300.

[13] P. Gordan, Über die auflösung linearer gleichungen mit reellen coefficienten, Math. Ann. **6** (1873), no. 1, 23–28.

[14] R. Hemmecke, M. Köppe, P. Malkin, and M. Walter, 4ti2– a software package for algebraic, geometric and combinatorial problems on linear spaces, available at www.4ti2.de.

[15] C. Kelley and D. Sridhara, Pseudocodewords of Tanner graphs, IEEE Trans. Inform. Theory **53** (2007), no. 11, 4013–4038.

[16] C. Kelley, D. Sridhara, and J. Rosenthal. Pseudocodeword weights for non-binary LDPC codes. Proc. IEEE Int. Symp. Inf. Theory, July 9-14, 2006, Seattle, USA.

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

[18] R. Koetter and P. O. Vontobel, Graph covers and iterative decoding of finite-length codes, Proc. 3rd Int. Symp. on Turbo Codes & Related Topics, Brest, France, pp. 75-82, Sep. 1-5, 2003.

[19] W. Kositwattanarerk and G. L. Matthews, Lifting the fundamental cone and enumerating the pseudocodewords of a parity-check code, IEEE Trans. Inform. Theory **57** (2011), no. 2, 898-909.

[20] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, Factor graphs and the sum-product algorithm, IEEE Trans. Inform. Theory **47** (2001), no. 2, pp. 498–519.

[21] M. Punekar, P.O. Vontobel, and M.F. Flanagan, Low-complexity LP decoding of nonbinary linear codes, IEEE Trans. Comm. **61**(2013), no. 8, pp. 3073-3085.

[22] V. Skachek, Characterization of graph-cover pseudocodewords of codes over $\mathbb{F}_3$, Proc. IEEE Inform. Theory Workshop, Dublin, Ireland, IEEE (2010).

[23] V. Skachek and M. F. Flanagan, Lower bounds on the minimum pseudodistance for linear codes with q-ary PSK modulation over AWGN, Proc. 5th Int. Symp. on Turbo Codes & Related Topics, Lausanne, Switzerland, September 2008.

[24] V. Skachek, M.F. Flanagan, E. Byrne, M. Greferath, Polytope representations for linear-programming decoding of non-binary linear codes, Proc. IEEE Int. Symp. on Inf. Theory, Toronto, Canada, July 2008.

[25] P.O. Vontobel and R. Koetter, Lower bounds on the minimum pseudo-weight of linear codes, Proc. IEEE Int. Symp. Inf. Theory, June 27 - July 2, 2004, Chicago, IL, USA.

[26] P.O. Vontobel and R. Koetter, Graph-cover decoding and finite-length analysis of message-passing iterative decoding of LDPC codes, CoRR, 2005, http://arxiv.org/abs/cs/0512078/.

[27] N. Wiberg, Codes and decoding on general graphs, Ph.D. dissertation, Linköping University, Linköping, Sweden, 1996.

[28] S.-T. Xia and F.-W. Fu, Minimum pseudo-codewords of LDPC codes, in Proc. IEEE Inf. Theory Workshop, Chengdu, China, Oct. 2006, pp. 109113.

[29] K. Yang, X. Wang, and J. Feldman, Cascaded formulation of the fundamental polytope of general linear block codes, Proc. IEEE Int. Symp. Inf. Theory, June 2007, pp. 1361–1365, Nice, France.

Wittawat Kositwattanarerk received the B.A. degrees in mathematics and economics from the University of Virginia, Charlottesville, in 2006 and the Ph.D. degree in mathematical sciences from Clemson University, Clemson, in 2011. After his postdoctoral work at Nanyang Technological University, he joined the the Department of Mathematics at Mahidol University as faculty. His research interest is in algebraic coding theory, in particular lattice codes and low-density parity-check (LDPC) codes.

Gretchen L. Matthews is Professor in the Department of Mathematical Sciences at Clemson University. She earned the B.S. degree in mathematics from Oklahoma State University in 1995 and the Ph.D. degree in mathematics from Louisiana State University in 1999. Following postdoctoral work at the University of Tennessee, she joined the faculty in the Department of Mathematical Sciences at Clemson University in 2001. Her research interests include algebra and its applications.

Copyright (c) 2014 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.