Lifting the Fundamental Cone and Enumerating the Pseudocodewords of a Parity-Check Code

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

Dedicated to the memory of Ralf Koetter (1963–2009)

***Abstract*—The performance of message-passing iterative decoding and linear programming decoding depends on the Tanner graph representation of the code. If the underlying graph contains cycles, then such algorithms could produce a noncodeword output. The study of pseudocodewords aims to explain this noncodeword output. We examine the structure of the pseudocodewords and show that there is a one-to-one correspondence between graph cover pseudocodewords and integer points in a lifted fundamental cone. This gives a simple proof that the generating function of the pseudocodewords for a general parity-check code is rational (a fact first proved by Li, Lu, and Wang (Lecture Notes in Computer Science, vol. 5557, 2009) via other methods). Our approach yields algorithms for producing this generating function and provides tools for studying the irreducible pseudocodewords. Specifically, Barvinok's algorithm and the Barvinok-Woods projection algorithm are applied, and irreducible pseudocodewords are found via a Hilbert basis for the lifted fundamental cone.**

***Index Terms*—Fundamental cone, irreducible pseudocodewords, iterative decoding, linear programming (LP) decoding, low-density parity-check (LDPC) code, pseudocodewords.**

I. Introduction

CODING theory allows messages to be transmitted and information to be stored and retrieved without suffering from loss and alteration of data. A decoding algorithm seeks to uncover the original message when a possibly erroneous message is received. In this paper, we focus on linear programming (LP) decoding. For low-density parity-check (LDPC) codes, the performance of LP decoding is near that of iterative message-passing algorithms. In fact, Koetter and Vontobel [33] provide a link between LP decoding and iterative message-passing algorithms via graph cover decoding. While LP decoding may correct beyond half the minimum distance of the code, it may output an illegitimate codeword. There have been many attempts to study the behavior of iterative decoders and their noncodeword outputs [10], [20]–[23]. In [23], Koetter and Vontobel introduce an object called the fundamental cone which contains all (scaled linear programming, or, equivalently, nonscaled graph cover) pseudocodewords. In [21] and [22], Koetter, Li, Vontobel, and Walker characterize all the pseudocodewords within this cone and prove that the pseudocodewords of a cycle code correspond to the monomials appearing (with nonzero coefficient) in an expansion of a rational function, specifically the edge zeta function of the normal graph of the code. In addition, they suggest as a goal determining such a rational function for a general parity-check code.

In this paper, methods from discrete geometry are exploited to give a rational generating function for the pseudocodewords of a general parity-check code and to provide tools to study pseudocodewords. We introduce a lifted fundamental cone $\hat{\mathcal{K}}$; the fundamental cone mentioned above is a projection of $\hat{\mathcal{K}}$. The lifted cone has the advantage that its integer points are precisely the pseudocodewords. This gives a simple proof that the generating function of the pseudocodewords of a general parity-check code is rational, a fact first proved by Li et al. [27]. Our approach differs from that of [27] in that we use the lifted fundamental cone and appeal to monomial substitution methods of Barvinok and Woods [5] while they rely on generators of the fundamental cone with even entries. The methods presented here yield algorithms for producing this generating function; moreover, the input into these algorithms is the lifted fundamental cone described in terms of inequalities rather than by its extreme rays. In particular, Barvinok's algorithm, a breakthrough polynomial-time algorithm to count lattice points in a rational polytope of a given dimension [2], is utilized here. Because Barvinok's algorithm (and subsequent improvements) have been implemented in software such as LattE [12], Barvinok 0.27 [31], and LattE macchiato [24], this perspective gives rise to computational tools to study pseudocodewords. In addition, the lifted fundamental cone provides a framework for studying the irreducible pseudocodewords. Irreducible pseudocodewords are found via a Hilbert basis for $\hat{\mathcal{K}}$; such pseudocodewords are especially important as the pseudoweight of any pseudocodeword is bounded below by the minimum pseudoweight of its irreducible pseudocodeword components.

This paper is organized as follows. This section concludes with a summary of notation. Section II provides a brief discussion of pseudocodewords of binary linear codes. The lifted fundamental cone is introduced in Section III. In Section IV, generating functions for the pseudocodewords and irreducible pseudocodewords are investigated; Barvinok's algorithm and the Barvinok-Woods projection algorithm are applied. The paper concludes with examples in Section V and final discussion in Section VI.

Manuscript received April 14, 2010; revised August 19, 2010; accepted October 26, 2010. Date of current version January 19, 2011. This work was supported by NSF DMS-0901693.

This paper is part of the special issue on "Facets of Coding Theory: From Algorithms to Networks," dedicated to the scientific legacy of Ralf Koetter.

The authors are with the Department of Mathematical Sciences, Clemson University, Clemson, SC 29634-0975 USA (e-mail: wkositw@clemson.edu; gmatthe@clemson.edu).

Communicated by G. D. Forney, Jr., Associate Editor for the special issue on "Facets of Coding Theory: From Algorithms to Networks."

Digital Object Identifier 10.1109/TIT.2010.2095071

Notation: The finite field with two elements is denoted $\mathbb{F}_2 = \{0,1\}$. 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 all $m \times n$ matrices with entries in $\mathbb{F}_2$ is denoted $\mathbb{F}_2^{m\times n}$, and $\mathbb{F}_2^n := \mathbb{F}_2^{1\times n}$. Similarly, $\mathbb{R}^n := \mathbb{R}^{1\times n}$ denotes the set of all $1 \times n$ matrices (that is, $1 \times n$ vectors) with entries in $\mathbb{R}$. Given a matrix $H \in \mathbb{F}_2^{m\times n}$, h_{ji} denotes the entry of H in the jth row and ith column, $\mathrm{Row}_j(H)$ denotes the jth row of H, and H^T denotes the transpose of H. The ith coordinate of a vector $\mathbf{v} \in \mathbb{R}^n$ is denoted v_i. Given $\mathbf{u} \in \mathbb{Z}^n$, the vector $\mathbf{x}^{\mathbf{u}}$ is defined as $\mathbf{x}^{\mathbf{u}} := x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n}$.

We adopt the usual coding theory terminology and notation. A binary linear code C of length n and dimension k is a subspace of $\mathbb{F}_2^n$ of dimension k; we use the term code to mean binary 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 binary matrix $H \in \mathbb{F}_2^{r\times n}$ such that C is then the null space of H; that is, an element $\mathbf{y} \in \mathbb{F}_2^n$ is a codeword of C if and only if $H\mathbf{y}^T = \mathbf{0} \in \mathbb{F}_2^{r\times 1}$. A parity-check matrix of a code is not unique. Since the performance of message-passing iterative decoding 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.

An algorithm is said to be polynomial time provided its running time is upperbounded by a polynomial in the input size of the algorithm. The input size of $a \in \mathbb{Z}$, denoted by $\chi(a)$, is the number of bits needed to express a in binary. In keeping with the references used throughout this paper, one may take $\chi(a)$ to be approximately $1 + \log|a|$. However, to also take into account the number of bits required to describe $\log|a|$, it may be more desirable to take $\chi(a)$ to be $1 + \log|a| + O(\log\log|a|)$. All complexity estimates in this paper will be given in terms of $\chi(a)$. Here and throughout the paper, the logarithm is taken base 2.

II. Preliminaries

In this paper, we assume a memoryless binary-input symmetric-output channel. The maximum likelihood (ML) decoding problem for a code C of length n can be stated as follows: Given a received word $\mathbf{w}$, find $\mathbf{y} \in C$ that maximizes $P(\mathbf{w} \mid \mathbf{y})$, the probability that $\mathbf{w}$ is received given that $\mathbf{y}$ is the transmitted codeword. This can be rephrased as a linear program (LP). To do so, consider the code C as implicitly embedded in $\mathbb{R}^n$ and let

$$\mathrm{poly}(C) := \left\{ \sum_{\mathbf{y}\in C} \lambda_{\mathbf{y}} \mathbf{y} \;\middle|\; \lambda_{\mathbf{y}} \geq 0, \sum_{\mathbf{y}\in C} \lambda_{\mathbf{y}} = 1 \right\} \subseteq [0,1]^n$$

denote the codeword polytope of C, meaning the convex hull of the codewords of C. Let

$$\gamma_i := \log\left(\frac{P(w_i \mid y_i = 0)}{P(w_i \mid y_i = 1)}\right)$$

denote the log-likelihood ratio at the i^{th} coordinate. Then the ML decoding problem is equivalent to

$$\text{minimize} \sum_{i=1}^{n} \gamma_i f_i \text{ subject to } \mathbf{f} \in \mathrm{poly}(C).$$

Unfortunately, solving this linear program is not practical for codes of reasonable block length; the description of the constraints determined by $\mathrm{poly}(C)$ is (typically) exponential in the block length. In an effort to make this problem more computationally feasible, Feldman, Wainwright, and Karger [14] replace the codeword polytope with a relaxed polytope

$$Q(H) := \bigcap_{j=1}^{r} \mathrm{poly}(C(\mathrm{Row}_j(H)))$$

which is the intersection of the codeword polytopes of the r simple parity-check codes defined by the rows of a parity-check matrix $H \in \mathbb{F}_2^{r\times n}$ of C. Then

$$\mathrm{poly}(C) \subseteq Q(H)$$

and $Q(H)$ has a more tractable representation than the original codeword polytope. This yields a relaxation of the original LP to what is called the Linear Code Linear Program

$$\text{minimize} \sum_{i=1}^{n} \gamma_i f_i \text{ subject to } \mathbf{f} \in Q(H).$$

The associated decoder is called an LP decoder. It may be that

$$\mathrm{poly}(C) \subsetneqq Q(H),$$

in which case the LP decoder is suboptimal. Indeed, this decoding rule may yield a vertex of $Q(H)$ that is not in $\mathrm{poly}(C)$, meaning a word that is not a codeword of $C = C(H)$. Hence, the vertices of $Q(H)$ are called LP pseudocodewords.

Pseudocodewords may also be described in terms of graph covers. Given a binary code $C(H)$, the binary matrix H also defines a bipartite graph $T(H)$ which is the graph with biadjacency matrix H. The graph $T(H)$, which is the bipartite representation of H, is called the Tanner graph due to [30]. The vertex set of $T(H)$ is $X \cup F$, where $X = \{x_1, \ldots, x_n\}$ is the set of bit nodes and $F = \{f_1, \ldots, f_r\}$ is the set of check nodes; one may think of the vertex x_i as corresponding to the ith column of H and the vertex f_j as corresponding to the jth row of H. The edge set of $T(H)$ is

$$E := \{\{x_i, f_j\} \mid h_{ji} \neq 0\}.$$

Notice that $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ is a codeword of $C(H)$ if and only if the binary value assignment $(c_1, c_2, \ldots, c_n)$ to the bit nodes of the Tanner graph $T(H)$ makes the binary sum of the values at the neighbors of every check node zero. A finite cover of $T(H)$ is a bipartite graph G such that there exists an integer m so that for each vertex $v \in X \cup F$, there is a set of vertices $\{v_1, \ldots, v_m\}$ of G with $\deg v = \deg v_i$ for all $1 \leq i \leq m$ and for every edge $\{u, v\} \in E$ there are m edges from the vertices in $\{u_1, \ldots, u_m\}$ to the vertices in $\{v_1, \ldots, v_m\}$ connected in

a 1–1 manner. A graph cover pseudocodeword of $C(H)$ is a vector $\mathbf{p} = (p_1, \ldots, p_n) \in \mathbb{Z}^n$ such that there is a finite cover of $T(H)$ which has $\tilde{\mathbf{c}}$ as a codeword and $p_i = \sum_{j=1}^{m} \tilde{c}_{ij}$, where $\tilde{c}_{i1}, \ldots, \tilde{c}_{im}$ are the values assigned to the m copies of the bit node x_i in the cover of $T(H)$.

Given a code $C(H)$, each LP pseudocodeword of $C(H)$ is a (scaled) graph cover pseudocodeword of $C(H)$, and each (scaled) graph cover pseudocodeword is a rational point in $Q(H)$ [33]. Here, we use the term *pseudocodeword* to refer to a graph cover pseudocodeword. Throughout, $\mathsf{PC}(H)$ denotes the set of pseudocodewords of the code $C(H)$. Lastly, 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 $\mathrm{Irr}(H)$ the set of all irreducible pseudocodewords of $C(H)$. It is known that irreducible pseudocodewords are the building blocks for $\mathsf{PC}(H)$ in that any pseudocodeword can be written as a sum of irreducible pseudocodewords. Characterizing them immediately provides much information about $\mathsf{PC}(H)$ [1], [20]. Irreducible pseudocodewords are not to be confused with minimal pseudocodewords. The minimal pseudocodewords of a code $C(H)$ are typically taken to be those $\mathbf{v}$ such that $\{\alpha\mathbf{v} : \alpha \in \mathbb{R}, \alpha \geq 0\}$ is an edge of the fundamental cone

$$\mathcal{K}(H) = \left\{ \mathbf{v} \in \mathbb{R}^n \;\middle|\; \begin{array}{l} v_i \geq 0 \text{ and} \\ \sum_{l=1, l\neq i}^{n} h_{jl} v_l \geq h_{ji} v_i \\ \forall 1 \leq i \leq n, 1 \leq j \leq r \end{array} \right\}.$$

The set $\mathrm{Irr}(H)$ contains a multiple of each minimal pseudocodeword of $C(H)$, but not every irreducible pseudocodeword arises in this way.

In [22], the authors characterize the pseudocodewords of a code $C(H)$ as those integer points within the fundamental cone $\mathcal{K}(H)$ which satisfy the parity-check conditions imposed by the rows of H. More formally, their result may be stated as follows.

Proposition 2.1: ([22, Theorem 4.4]) Let $H \in \mathbb{F}_2^{r\times n}$. Given $\mathbf{p} \in \mathbb{Z}^n$, the following are equivalent:

1) $\mathbf{p}$ is a pseudocodeword of the code $C(H)$;
2) $\mathbf{p} \in \mathcal{K}(H)$ and $H\mathbf{p}^T = \mathbf{0} \bmod 2$.

In this same paper, it is shown that the pseudocodewords of a cycle code, meaning a code given by a parity-check matrix having exactly two nonzero entries in each column, are precisely the exponent vectors of monomials appearing with nonzero coefficient in the Taylor series expansion of a certain rational function. More precisely, they prove the following result.

Proposition 2.2: ([22, Theorem 5.9]) Let $H \in \mathbb{F}_2^{r\times n}$ be a matrix with exactly two nonzero entries in each column. Then the following are equivalent:

1) $\mathbf{p}$ is a pseudocodeword of the code $C(H)$;
2) $\mathbf{x}^{\mathbf{p}}$ appears with nonzero coefficient in $\zeta_{N(H)}(\mathbf{x})$, the edge zeta function of the normal graph of $T(H)$.

It is left open to determine a similar function for a general parity-check code. Here, we set out to show that the generating function for the pseudocodewords of a general parity-check code is a rational function (a fact originally proved in [27]) which has a compact rational form, give methods to yield this form, and provide tools for investigating the pseudocodewords. To do this, we introduce the lifted fundamental cone in the next section.

III. The Lifted Fundamental Cone

In this section, we define the lifted fundamental cone of a parity-check code and relate it to the fundamental cone and the set of irreducible pseudocodewords.

Definition 3.1: Given $H \in \mathbb{F}_2^{r\times n}$, the lifted fundamental cone of $C(H)$ is

$$\hat{\mathcal{K}}(H) = \left\{ (\mathbf{v}, \mathbf{a}) \in \mathbb{R}^{n+r} \;\middle|\; \begin{array}{l} v_i \geq 0, H\mathbf{v}^T = 2\mathbf{a}^T, \text{and} \\ \sum_{l=1}^{n} h_{jl} v_l \geq 2 h_{ji} v_i \\ \forall 1 \leq i \leq n, 1 \leq j \leq r \end{array} \right\}.$$

Notice that the use of the vector $\mathbf{a}$ in Definition 3.1 is similar to that in the reformulation of ML decoding as an integer programming problem in [8].

To relate the lifted cone $\hat{\mathcal{K}}(H)$ to the fundamental cone $\mathcal{K}(H)$, define the projection

$$\begin{array}{rccc} \pi: & \mathbb{R}^{n+r} & \to & \mathbb{R}^n \\ & (\mathbf{v}, \mathbf{a}) & \mapsto & \mathbf{v}. \end{array} \tag{1}$$

We make the relationship between the lifted fundamental cone and the pseudocodewords precise in the following proposition.

Proposition 3.2: Let $H \in \mathbb{F}_2^{r\times n}$. The projection $\pi|_{\hat{\mathcal{K}}(H)}$ is one-to-one and

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

Furthermore

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

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

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

$$2\mathbf{a}^T = H\mathbf{v}^T = H\mathbf{v}'^T = 2\mathbf{a}'^T.$$

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

Now

$$\begin{aligned} \pi(\hat{\mathcal{K}}(H)) &= \left\{ \mathbf{v} \in \mathbb{R}^n \;\middle|\; \begin{array}{l} v_i \geq 0, H\mathbf{v}^T = 2\mathbf{a}^T \\ \text{for some } \mathbf{a} \in \mathbb{R}^r, \text{and} \\ \sum_{l=1}^{n} h_{jl} v_l \geq 2 h_{ji} v_i \\ \forall 1 \leq i \leq n, 1 \leq j \leq r \end{array} \right\} \\ &= \left\{ \mathbf{v} \in \mathbb{R}^n \;\middle|\; \begin{array}{l} v_i \geq 0 \text{ and} \\ \sum_{l=1}^{n} h_{jl} v_l \geq 2 h_{ji} v_i \\ \forall 1 \leq i \leq n, 1 \leq j \leq r \end{array} \right\} \\ &= \mathcal{K}(H) \end{aligned}$$

where the last equality follows from the definition of fundamental cone.

Let $(\mathbf{v}, \mathbf{a})$ be an integer point in $\hat{\mathcal{K}}(H)$. Then

$$\mathbf{v} = \pi(\mathbf{v}, \mathbf{a}) \in \mathcal{K}(H)$$

and $H\mathbf{v}^T = 2\mathbf{a}^T$ implying that $H\mathbf{v}^T = \mathbf{0} \bmod 2$. By Proposition 2.1, $\pi(\mathbf{v}, \mathbf{a}) = \mathbf{v}$ is a pseudocodeword of $C(H)$. On the other hand, let $\mathbf{p} \in \mathsf{PC}(H)$. Then $\mathbf{p}$ is an integer vector in $\mathcal{K}(H)$ such that $H\mathbf{p}^T = \mathbf{0} \bmod 2$. Since $\pi(\hat{\mathcal{K}}(H)) = \mathcal{K}(H)$, $(\mathbf{p}, \mathbf{a}) \in \hat{\mathcal{K}}(H)$ for some $\mathbf{a} \in \mathbb{R}^r$. Then $H\mathbf{p}^T = \mathbf{0} \bmod 2$ implies $\mathbf{a} \in \mathbb{Z}^r$. We conclude that $\pi(\hat{\mathcal{K}}(H) \cap \mathbb{Z}^{n+r}) = \mathsf{PC}(H)$. ■

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 called *pointed* if it has a vertex at the origin. The set of integer vectors in a pointed rational cone forms an additive semigroup. The minimal set of generators $\mathcal{B}$ of this semigroup is finite [15] and unique [11]; $\mathcal{B}$ 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

$$\left\{ \lambda_1\mathbf{b}_1 + \cdots + \lambda_t\mathbf{b}_t \,\middle|\, \begin{array}{l} \lambda_1, \ldots, \lambda_t \geq 0 \\ \text{and } \lambda_1, \ldots, \lambda_t \in \mathbb{Z} \end{array} \right\} = K \cap \mathbb{Z}^n.$$

We relate the Hilbert basis of $\hat{\mathcal{K}}(H)$ and the irreducible pseudocodewords of $C(H)$ in the following proposition.

Proposition 3.3: Let $H \in \mathbb{F}_2^{r \times n}$. The set of irreducible pseudocodewords of $C(H)$ is

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

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

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

Let $\mathbf{p} \in \mathrm{Irr}(H)$ be an irreducible pseudocodeword of $C(H)$. It follows from Proposition 3.2 that $\mathbf{p} = \pi(\mathbf{y})$ for some $\mathbf{y} \in \hat{\mathcal{K}}(H) \cap \mathbb{Z}^{n+r}$. Since $\mathcal{B}$ is a Hilbert basis for $\hat{\mathcal{K}}(H)$, $\mathbf{y} = \sum_{i=1}^{t} \lambda_i \mathbf{b}_i$ 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 3.2, 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 $\mathrm{Irr}(H) \subseteq \pi(\mathcal{B})$.

Now consider $\pi(\mathbf{b})$ where $\mathbf{b} \in \mathcal{B}$. Then $\mathbf{b} \in \hat{\mathcal{K}}(H) \cap \mathbb{Z}^{n+r}$. Hence, $\pi(\mathbf{b})$ is a pseudocodeword by Proposition 3.2. 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 3.2, $\mathbf{p}_1 = \pi(\mathbf{p}_1, \mathbf{a}_1)$ and $\mathbf{p}_2 = \pi(\mathbf{p}_2, \mathbf{a}_2)$ where $(\mathbf{p}_1, \mathbf{a}_1)$, $(\mathbf{p}_2, \mathbf{a}_2) \in \hat{\mathcal{K}}(H)$. 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 $\pi(\mathcal{B}) \subseteq \mathrm{Irr}(H)$. ■

IV. Enumerating Pseudocodewords

The lifted fundamental cone was introduced in the previous section. In this section, we use the lifted fundamental cone to study $\sum_{\mathbf{p} \in \mathsf{PC}(H)} \mathbf{x}^{\mathbf{p}}$, the generating function for the pseudocodewords of the code $C(H)$, as well as $\sum_{\mathbf{p} \in \mathrm{Irr}(H)} \mathbf{x}^{\mathbf{p}}$, the generating function for the irreducible pseudocodewords of $C(H)$.

A. The Generating Function for Pseudocodewords

We begin this subsection by addressing a question from [22]. Our approach relies on the lifted fundamental cone; for an alternate proof, see [27, Theorem 13].

Theorem 4.1: Let $H \in \mathbb{F}_2^{r \times n}$. The generating function of the pseudocodewords of $C(H)$ is a rational function.

Proof: It is well-known that the generating function of a pointed rational cone is rational ([29, Theorem 4.6.11]). Thus, the generating function for the integer points in the lifted fundamental cone

$$f(x_1, x_2, \ldots, x_{n+r}) := \sum_{(\mathbf{v}, \mathbf{a}) \in \hat{\mathcal{K}}(H) \cap \mathbb{Z}^{n+r}} \mathbf{x}^{(\mathbf{v}, \mathbf{a})},$$

is rational. Here, $\mathbf{x} \in \mathbb{C}^{n+r}$.

Since $(x_1, \ldots, x_n, 1, \ldots, 1)$ is not a pole of any fraction appearing in the rational expression of f (see [29, Proposition 4.6.10, Theorem 4.6.11]), it follows that:

$$\begin{aligned} f(x_1, \ldots, x_n, 1, \ldots, 1) &= \sum_{(\mathbf{v}, \mathbf{a}) \in \hat{\mathcal{K}}(H) \cap \mathbb{Z}^{n+r}} \mathbf{x}^{\mathbf{v}} \\ &= \sum_{\mathbf{v} \in \pi(\hat{\mathcal{K}}(H) \cap \mathbb{Z}^{n+r})} \mathbf{x}^{\mathbf{v}} \\ &= \sum_{\mathbf{v} \in \mathsf{PC}(H)} \mathbf{x}^{\mathbf{v}} \end{aligned}$$

is rational where $\mathbf{x} \in \mathbb{C}^n$. ■

The proof of Theorem 4.1 employs the rational form of the generating function of the integer points in the lifted fundamental cone. Alternatively, one may appeal to the method of monomial substitution (or, specialization of rational functions) due to Barvinok and Woods detailed below. The significance of this approach is that such a substitution may be carried out efficiently.

Lemma 4.2: ([5, Theorem 2.6]) Given a rational function

$$f(\mathbf{x}) = \sum_{i \in I} \alpha_i \frac{\mathbf{x}^{\mathbf{a}_i}}{(1-\mathbf{x}^{\mathbf{u}_{i1}}) \cdots (1-\mathbf{x}^{\mathbf{u}_{is}})} \tag{2}$$

where I is a finite set, $\alpha_i \in \mathbb{Q}$, $\mathbf{a}_i, \mathbf{u}_{ij} \in \mathbb{Z}^n$, and $\mathbf{u}_{ij} \neq \mathbf{0}$ for all i, j, and a monomial map

$$\begin{array}{rccc} \phi: & \mathbb{C}^d & \rightarrow & \mathbb{C}^n \\ & \mathbf{z} & \mapsto & \left(\mathbf{z}^{\mathbf{l}_1}, \ldots, \mathbf{z}^{\mathbf{l}_n}\right) \end{array} \tag{3}$$

where $\mathbf{l}_1, \ldots, \mathbf{l}_n \in \mathbb{Z}^d$ such that the image of ϕ does not lie entirely in the set of poles of $f(\mathbf{x})$, there is a polynomial time algorithm which computes $f(\phi(\mathbf{z}))$ in the form

$$f(\phi(\mathbf{z})) = \sum_{i \in I'} \beta_i \frac{\mathbf{z}^{\mathbf{b}_i}}{(1-\mathbf{z}^{\mathbf{w}_{i1}}) \cdots (1-\mathbf{z}^{\mathbf{w}_{it}})}$$

where $t \leq s$, I' is a finite set, $\beta_i \in \mathbb{Q}$, $\mathbf{b}_i, \mathbf{w}_{ij} \in \mathbb{Z}^d$, and $\mathbf{w}_{ij} \neq \mathbf{0}$ for all i, j.

As in the proof of Theorem 4.1, let

$$f(x_1, x_2, \ldots, x_{n+r}) \coloneqq \sum_{(\mathbf{v},\mathbf{a}) \in \hat{\mathcal{K}}(H) \cap \mathbb{Z}^{n+r}} \mathbf{x}^{(\mathbf{v},\mathbf{a})}$$

be the generating function of the integer points in the lifted fundamental cone $\hat{\mathcal{K}}(H)$ where $H \in \mathbb{F}_2^{r \times n}$. Then one may apply Lemma 4.2 to obtain $f(x_1, \ldots, x_n, 1, \ldots, 1)$. Take

$$\mathbf{l}_i = \begin{cases} \mathbf{e}_i & \text{if } 1 \leq i \leq n \\ \mathbf{0} & \text{if } n+1 \leq i \leq n+r \end{cases}$$

where $\mathbf{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ is the vector with 1 in the ith coordinate and 0's elsewhere. Then

$$f(\phi(\mathbf{z})) = f(x_1, x_2, \ldots, x_n, 1, 1, \ldots, 1)$$

may be found according to Lemma 4.2.

Remark 4.3: The algorithm in Lemma 4.2 takes as input the rational function f expressed as in (2) and the monomial map ϕ as in (3). The input size of ϕ is approximately

$$\sum_{i=1}^{n} \sum_{j=1}^{d} \chi(l_{ij})$$

and the input size of f is approximately

$$\sum_{i \in I} \left[\chi(b_i) + \chi(c_i) + \sum_{j=1}^{d} \left(\chi(a_{ij}) + \sum_{t=1}^{s} \chi(u_{itj}) \right) \right] \tag{4}$$

where $\alpha_i = \frac{b_i}{c_i}$ with $b_i, c_i \in \mathbb{Z}$.

Notice that Theorem 4.1 gives no information concerning the rational form of the generating function of the pseudocodewords other than its existence. To gain more insight into the rational form of this generating function, we may apply standard tools from discrete geometry. We recall these here for easy reference; for more background, see [4], [6], and [29].

Let $\mathbf{u}_1, \ldots, \mathbf{u}_k \in \mathbb{Z}^d$ be linearly independent integer vectors. The *simple rational cone* generated by $\mathbf{u}_1, \ldots, \mathbf{u}_k$ is the set

$$\mathcal{S} = \left\{ \sum_{i=1}^{k} \alpha_i \mathbf{u}_i \,\middle|\, \alpha_i \geq 0 \right\}.$$

If $k = d$, then $\mathcal{S}$ is said to be *full-dimensional*; if $k < d$, then $\mathcal{S}$ is called *lower-dimensional*. The vectors $\mathbf{u}_1, \ldots, \mathbf{u}_k$ are called the generators of $\mathcal{S}$. The *fundamental parallelepiped* of $\mathbf{u}_1, \ldots, \mathbf{u}_k$ is the set

$$\Pi = \left\{ \sum_{i=1}^{k} \alpha_i \mathbf{u}_i \,\middle|\, 0 \leq \alpha_i < 1 \right\}.$$

We sometimes write $\Pi(\mathcal{S})$ to mean the fundamental parallelepiped of the given generators of $\mathcal{S}$. The index of a simple rational cone $\mathcal{S}$, denoted $\mathrm{ind}(\mathcal{S})$, is the number of integer points in $\Pi(\mathcal{S})$. It can be easily proved that the index of $\mathcal{S}$ is the same as the volume of $\Pi(\mathcal{S})$ (see, for instance, [3, Theorem 2]). The following lemma describes the generating function for the integer points in a simple rational cone.

Lemma 4.4: ([29, Corollary 4.6.8]) For a simple rational cone $\mathcal{S}$ with generators $\mathbf{u}_1, \ldots, \mathbf{u}_k \in \mathbb{Z}^d$, we have

$$\sum_{\mathbf{m} \in \mathcal{S} \cap \mathbb{Z}^d} \mathbf{x}^{\mathbf{m}} = \frac{\sum_{\mathbf{m} \in \Pi(\mathcal{S}) \cap \mathbb{Z}^d} \mathbf{x}^{\mathbf{m}}}{(1-\mathbf{x}^{\mathbf{u}_1}) \cdots (1-\mathbf{x}^{\mathbf{u}_k})}.$$

The notion of a triangulation is especially useful in investigating the rational form of the generating function of the pseudocodewords. A triangulation of a pointed rational cone K is a finite set $\Gamma = \{S_1, \ldots, S_t\}$ of simple rational cones satisfying:

1) $\cup_{i=1}^{t} S_i = K$;
2) if $S \in \Gamma$, then every face of S is an element of Γ; and
3) for all $1 \leq i < j \leq t$, $S_i \cap S_j$ is a common face of S_i and S_j.

Theorem 4.5: Given a binary matrix $H \in \mathbb{F}_2^{r \times n}$, the generating function of the pseudocodewords of $C(H)$ may be expressed as

$$\sum_{\mathbf{p} \in \mathsf{PC}(H)} \mathbf{x}^{\mathbf{p}} = \frac{\sigma(\mathbf{x})}{(1-\mathbf{x}^{\mathbf{v}_1}) \cdots (1-\mathbf{x}^{\mathbf{v}_l})}$$

where $\mathbf{v}_1, \ldots, \mathbf{v}_l$ are integer vectors and $\sigma(\mathbf{x})$ is a polynomial.

Proof: The lifted fundamental cone $\hat{\mathcal{K}}(H)$ is clearly a pointed rational cone. According to [29, Lemma 4.6.1] (or [6, Theorem 3.2]), the lifted fundamental cone can be triangulated into a finite union of simple rational cones using no new generators, meaning that the generators of each simple rational cone are among the generators of $\hat{\mathcal{K}}(H)$. Hence, there exist simple rational cones $S_1, \ldots, S_t$ such that

$$\hat{\mathcal{K}}(H) = S_1 \cup \cdots \cup S_t$$

and the generators for each S_i are among the generators $\mathbf{w}_1, \ldots, \mathbf{w}_l$ of $\hat{\mathcal{K}}(H)$. Given $I \subseteq \{1, \ldots, t\}$, let

$$S_I \coloneqq \cap_{i \in I} S_i.$$

Then S_I is a simple rational cone, because the intersection of simple rational cones resulting from a triangulation is a simple rational cone (according to the definition of trianglation; see also [6, Exercise 3.2]). Hence, the generating function for the integer points of each S_I follows from Lemma 4.4. Applying inclusion-exclusion and Lemma 4.4, we obtain the generating function for the integer points of the lifted fundamental cone

$$\begin{aligned}&\sum_{\mathbf{m}\in\hat{\mathcal{K}}(H)\cap\mathbb{Z}^{n+r}} \mathbf{x}^{\mathbf{m}} \\ &\quad=\sum_{j=1}^{t}(-1)^{j-1}\left(\sum_{\substack{I\subseteq\{1,\ldots,t\}\\|I|=j}}\left(\sum_{\mathbf{m}\in S_I\cap\mathbb{Z}^{n+r}}\mathbf{x}^{\mathbf{m}}\right)\right) \\ &\quad=\sum_{j=1}^{t}(-1)^{j-1}\left(\sum_{\substack{I\subseteq\{1,\ldots,t\}\\|I|=j}}\frac{\sum_{\mathbf{m}\in\Pi(S_I)\cap\mathbb{Z}^{n+r}}\mathbf{x}^{\mathbf{m}}}{(1-\mathbf{x}^{\mathbf{u}_{I1}})\cdots(1-\mathbf{x}^{\mathbf{u}_{Il_I}})}\right)\end{aligned}$$

where $\mathbf{u}_{I1},\ldots,\mathbf{u}_{Il_I}$ are generators of S_I. Since for each subset $I\subseteq\{1,\ldots,t\}$, $\mathbf{u}_{I1},\ldots,\mathbf{u}_{Il_I}\in\{\mathbf{w}_1,\ldots,\mathbf{w}_l\}$, it follows that

$$\sum_{\mathbf{m}\in\hat{\mathcal{K}}(H)\cap\mathbb{Z}^{n+r}}\mathbf{x}^{\mathbf{m}}=\frac{\hat{\sigma}(\mathbf{x})}{(1-\mathbf{x}^{\mathbf{w}_1})\cdots(1-\mathbf{x}^{\mathbf{w}_l})}$$

where $\hat{\sigma}(\mathbf{x})$ is a polynomial.

Now, as in the proof of Theorem 4.1, set

$$f(x_1,\ldots,x_{n+r}):=\sum_{\mathbf{m}\in\hat{\mathcal{K}}(H)\cap\mathbb{Z}^{n+r}}\mathbf{x}^{\mathbf{m}}.$$

Then use Lemma 4.2 to obtain

$$\begin{aligned}\sum_{\mathbf{p}\in\mathsf{PC}(H)}\mathbf{x}^{\mathbf{p}}&=f(x_1,\ldots,x_n,1,\ldots,1)\\&=\frac{\sigma(\mathbf{x})}{(1-\mathbf{x}^{\mathbf{v}_1})\cdots(1-\mathbf{x}^{\mathbf{v}_l})}\end{aligned}$$

where $\sigma(\mathbf{x})$ is a polynomial and $\mathbf{v}_i=\pi(\mathbf{w}_i)\in\mathbb{Z}^n$ for all i, $1\le i\le l$. ∎

Remark 4.6:

1) The discussion in the proof of Theorem 4.5 is similar in spirit to that of [27, Theorem 13]. However, we apply this analysis to the lifted fundamental cone whereas they manipulate generators of the fundamental cone so that the entries are all even. Both approaches involve inclusion-exclusion; we exhibit the application of inclusion-exclusion explicitly above.
2) Consider the argument in the proof of Theorem 4.5 without the application of inclusion-exclusion. The result is a rational function whose expansion contains a monomial $\mathbf{x}^{(\mathbf{p},\mathbf{a})}$ with nonzero coefficient if and only if $\mathbf{p}$ is a pseudocodeword. This is demonstrated below.
   Let $H\in\mathbb{F}_2^{r\times n}$. Let $S_1,\ldots,S_t$ be a triangulation of $\hat{\mathcal{K}}(H)$ as in the proof of Theorem 4.5. Let
$$g(\mathbf{x})=\sum_{i=1}^{t}\sum_{\mathbf{m}\in S_i\cap\mathbb{Z}^{n+r}}\mathbf{x}^{\mathbf{m}}.$$
   Applying Lemma 4.4 gives
$$g(\mathbf{x})=\sum_{i=1}^{t}\frac{\sum_{\mathbf{m}\in\Pi(S_i)\cap\mathbb{Z}^{n+r}}\mathbf{x}^{\mathbf{m}}}{(1-\mathbf{x}^{\mathbf{u}_{i1}})\cdots(1-\mathbf{x}^{\mathbf{u}_{il_i}})}.$$
   Clearly, $g(\mathbf{x})$ is a rational function, and inclusion-exclusion is not required to produce this form. Moreover, a monomial with exponent vector $(\mathbf{p},\mathbf{a})$ appears with nonzero coefficient in a Taylor expansion of $g(\mathbf{x})$ if and only if $\mathbf{p}$ is a pseudocodeword of $C(H)$. Strictly speaking, $g(\mathbf{x})$ is not a generating function for the pseudocodewords of $C(H)$, because the expansion of $g(\mathbf{x})$ may contain nonzero coefficients that are integers other than 1. However, it is reminiscent of the edge zeta function related to a cycle code in Proposition 2.2. Allowing coefficients other than 0 and 1 has also proven useful in contexts such as [32]; there, a connection is established between the coefficients of the edge zeta function of a cycle code and the Bethe entropy. In the general case discussed here, no mathematical significance has been established. A function similar to $g(\mathbf{x})$ is mentioned in [27, Remark 1], though without the use of the lifted fundamental cone.

While Theorem 4.5 gives a specific form of the rational function guaranteed by Theorem 4.1, this approach is still lacking in some sense. Namely, it involves enumerating all the integer points in the fundamental parallelepipeds $\Pi(S_I)$; according to the discussion following [3, Theorem 1], the sums resulting from Lemma 4.4 while finite may be large. Moreover, direct application of inclusion-exclusion can be quite costly. In an effort to circumvent these difficulties (or deal with them more efficiently), we apply Barvinok's algorithm and its improvements. Introduced in 1994, Barvinok's algorithm is a polynomial time algorithm for counting the number of lattice points in a convex polyhedron in a fixed dimension [2]. It has seen applications in optimization, statistics, and algebra; here, we apply it to the enumeration of pseudocodewords of a general parity-check code.

Barvinok's algorithm was inspired by the fact that a long polynomial or infinite series can sometimes be written as a much shorter rational function. Consider, for instance

$$\sum_{m=0}^{\infty}x^m=\frac{1}{1-x}.$$

While $\sum_{m=0}^{\infty}x^m$ involves an infinite number of monomials, it can be written as $\frac{1}{1-x}$ which involves only three monomials. Because there are a number of excellent surveys of Barvinok's algorithm, its applications, and subsequent improvements [3]–[5], [7], [12], [25], [26], [31], we only mention those elements that seem relevant to the study of pseudocodewords.

A simple rational cone $\mathcal{S}$ is said to be *unimodular* if and only if $\mathrm{ind}(\mathcal{S})=1$. Notice that if $\mathcal{S}$ is unimodular, then $\mathbf{0}$ is the unique integer point in $\Pi(\mathcal{S})$. According to Lemma 4.4, if $\mathcal{S}$ is unimodular, then

$$\sum_{\mathbf{m}\in\mathcal{S}\cap\mathbb{Z}^d}\mathbf{x}^{\mathbf{m}}=\frac{1}{(1-\mathbf{x}^{\mathbf{u}_1})\cdots(1-\mathbf{x}^{\mathbf{u}_k})}\tag{5}$$

where $\mathbf{u}_1, \ldots, \mathbf{u}_k$ are generators of $\mathcal{S}$. The dual of a rational cone $K \subseteq \mathbb{R}^d$ is

$$K^* := \{\mathbf{x} \in \mathbb{R}^d \mid \mathbf{x}\mathbf{y}^T \geq 0 \, \forall \mathbf{y} \in K\}.$$

Hence, the dual of a rational cone is a rational cone, and

$$(K^*)^* = K$$

according to the Bipolar Theorem. Given a set $A \subseteq \mathbb{R}^d$, the indicator function of A is

$$\begin{array}{rccc} [A]: & \mathbb{R}^d & \rightarrow & \mathbb{R} \\ & \mathbf{m} & \mapsto & \begin{cases} 1 & \text{if } \mathbf{m} \in A \\ 0 & \text{if } \mathbf{m} \notin A. \end{cases} \end{array}$$

Generating functions of integer points in rational cones respect linear identities of their indicator functions [4, Theorem 3.1] as do the indicator functions of their duals [4, Corollary 2.8]; more precisely, given rational cones $K_1, \ldots, K_t \subseteq \mathbb{R}^d$ and $\alpha_1, \ldots, \alpha_t \in \mathbb{Q}$

$$\sum_{i=1}^{t} \alpha_i [K_i] = 0 \Rightarrow \quad \sum_{i=1}^{t} \alpha_i \sum_{\mathbf{m} \in K_i \cap \mathbb{Z}^d} \mathbf{x}^{\mathbf{m}} = 0 \tag{6}$$

and

$$\sum_{i=1}^{t} \alpha_i [K_i] = 0 \Rightarrow \quad \sum_{i=1}^{t} \alpha_i [K_i^*] = 0. \tag{7}$$

If a cone $K \subseteq \mathbb{R}^d$ contains a straight line, then we make the standard convention that $\sum_{\mathbf{m} \in K \cap \mathbb{Z}^d} \mathbf{x}^{\mathbf{m}} \equiv 0$.

Barvinok's algorithm provides an efficient method for decomposing a simple rational cone into simple rational cones with smaller indices, as detailed in the following lemma.

Lemma 4.7: ([2, Theorem 5.4]) Fix d. Given a simple rational cone $\mathcal{S} \subseteq \mathbb{R}^d$ described in terms of rational inequalities, there exists a polynomial time algorithm which computes a signed decomposition

$$[\mathcal{S}] = \sum_{i \in I_1} \epsilon_i [\mathcal{S}_i] + \sum_{i \in I_2} \epsilon_i [\mathcal{S}_i]$$

where $\epsilon_i \in \{-1, 1\}$, $\mathcal{S}_i$ is a simple rational cone, and

$$\operatorname{ind}(\mathcal{S}_i) < \operatorname{ind}(\mathcal{S})$$

for all $i \in I_1 \cup I_2$. Moreover, in this decomposition, the cones $\mathcal{S}_i$, $i \in I_1$, are full-dimensional whereas the cones $\mathcal{S}_i$, $i \in I_2$, are lower-dimensional.

Theorem 4.8: Fix $d := n + r$. Given $H \in \mathbb{F}_2^{r \times n}$, there exists a polynomial time algorithm which computes the generating function of the pseudocodewords of $C(H)$ as a finite sum

$$\sum_{\mathbf{p} \in \mathsf{PC}(H)} \mathbf{x}^{\mathbf{p}} = \sum_i \epsilon_i \frac{1}{(1 - \mathbf{x}^{\mathbf{v}_{i1}}) \cdots (1 - \mathbf{x}^{\mathbf{v}_{id}})}$$

where $\epsilon_i \in \{-1, 1\}$ and the $\mathbf{v}_{ij}$ are integer vectors for all i, j.

Proof: The proof is a straightforward application of Barvinok's algorithm with Brion's polarization trick (noted in the seminal paper [9]) to the lifted fundamental cone.

First, triangulate the dual of the lifted fundamental cone $\hat{\mathcal{K}}(H)^*$ to obtain simple rational cones $S_1^*, \ldots, S_t^*$. Next, apply the signed decomposition of Lemma 4.7 to each S_i^*. For each $i = 1, \ldots, t$, this gives

$$[S_i^*] = \sum_{j \in I_{i1}} \epsilon_{ij} [S_{ij}^*] + \sum_{j \in I_{i2}} \epsilon_{ij} [S_{ij}^*]. \tag{8}$$

Note that the index of S_{ij}^* is less than that of S_i^* for each index $j \in I_{i1} \cup I_{i2}$.

We claim that the lower-dimensional simple rational cones S_{ij}^*, $j \in I_{i2}$, may be safely discarded with no effect on the generating function of the integer points in S_i. To see this, polarize Equation (8) back. Applying (7) gives

$$[S_i] = \sum_{j \in I_{i1}} \epsilon_{ij} [S_{ij}] + \sum_{j \in I_{i2}} \epsilon_{ij} [S_{ij}].$$

Now, according to (6)

$$\begin{aligned} \sum_{\mathbf{m} \in S_i \cap \mathbb{Z}^d} \mathbf{x}^{\mathbf{m}} &= \sum_{j \in I_{i1}} \epsilon_{ij} \sum_{\mathbf{m} \in S_{ij} \cap \mathbb{Z}^d} \mathbf{x}^{\mathbf{m}} \\ &\quad + \sum_{j \in I_{i2}} \epsilon_{ij} \sum_{\mathbf{m} \in S_{ij} \cap \mathbb{Z}^d} \mathbf{x}^{\mathbf{m}} \\ &= \sum_{j \in I_{i1}} \epsilon_{ij} \sum_{\mathbf{m} \in S_{ij} \cap \mathbb{Z}^d} \mathbf{x}^{\mathbf{m}} \end{aligned}$$

as the dual of a lower-dimensional simple rational cone contains a straight line and so

$$\sum_{\mathbf{m} \in S_{ij} \cap \mathbb{Z}^d} \mathbf{x}^{\mathbf{m}} \equiv 0$$

for each $j \in I_{i2}$. Hence, the claim holds and there is no need to keep track of the cones S_{ij}^* with $j \in I_{i2}$ (or their duals).

Iterate this procedure, applying Lemma 4.7 next to the S_{ij}^* with $j \in I_{i1}$. Each time, the indices of the simple rational cones obtained decrease (doubly exponentially [4]). Continue until a decomposition

$$[S_i^*] = \sum_{j \in I_i} \epsilon_{ij} [C_{ij}^*] \mod \begin{array}{l} \text{indicators of lower–} \\ \text{dimensional cones} \end{array}$$

is obtained with all C_{ij}^* unimodular. Then

$$[S_i] = \sum_{j \in I_i} \epsilon_{ij} [C_{ij}] \mod \begin{array}{l} \text{indicators of} \\ \text{cones containing} \\ \text{straight lines} \end{array} \tag{9}$$

and all C_{ij} are unimodular being duals of unimodular cones [4]. It follows that

$$[\hat{\mathcal{K}}(H)] = \sum_{i \in I} \epsilon_i [K_i] \mod \begin{array}{l} \text{indicators of} \\ \text{cones containing} \\ \text{straight lines} \end{array}$$

where each cone K_i, $i \in I$, is unimodular. Then Equations (6) and (5) imply that

$$\sum_{\mathbf{m} \in \hat{\mathcal{K}}(H) \cap \mathbb{Z}^d} \mathbf{x}^{\mathbf{m}} = \sum_{i \in I} \epsilon_i \frac{1}{(1 - \mathbf{x}^{\mathbf{w}_{i1}}) \cdots (1 - \mathbf{x}^{\mathbf{w}_{id}})}$$

where $\mathbf{w}_{i1}, \ldots, \mathbf{w}_{id}$ are generators of K_i.

Finally, to extract the generating function for the pseudocodewords of $C(H)$, set

$$f(x_1, \ldots, x_d) := \sum_{\mathbf{m} \in \hat{\mathcal{K}}(H) \cap \mathbb{Z}^d} \mathbf{x}^{\mathbf{m}}$$

and use Lemma 4.2 to obtain

$$\begin{aligned} \sum_{\mathbf{p} \in \mathsf{PC}(H)} \mathbf{x}^{\mathbf{p}} &= f(x_1, \ldots, x_n, 1, \ldots, 1) \\ &= \sum_{i \in I} \epsilon_i \frac{1}{(1 - \mathbf{x}^{\mathbf{v}_{i1}}) \cdots (1 - \mathbf{x}^{\mathbf{v}_{id}})} \end{aligned}$$

where $\mathbf{v}_{ij} = \pi(\mathbf{w}_{ij}) \in \mathbb{Z}^n$ for all $i \in I$ and $1 \leq j \leq d$. ■

Remark 4.9:

1) Barvinok's algorithm takes as input a pointed rational cone described in terms of rational inequalities. Hence, one does not have to determine the extreme rays of the cone which are not typically available *a priori*.
2) The complexity of Barvinok's algorithm applied as described in the proof of Theorem 4.8 is $\mathcal{L}^{O(n+r)}$, where $\mathcal{L}$ is the input size of $\hat{\mathcal{K}}(H)$. The input size $\mathcal{L}$ is approximately

$$(r + \delta r)(n + r + 2)$$

where δ denotes the maximum number of nonzero entries in each row of the parity check matrix H. The number of cones associated with each set I_{i1} is at most $n + r$. The monomial substitution may also be done in polynomial time according to Lemma 4.2. Note that Barvinok's algorithm is polynomial with respect to the input size assuming the dimension is fixed. However, as the dimension of the lifted fundamental cone grows with the length of the code and the size of the parity check matrix, the algorithm is not polynomial with respect to the length of the code. While these complexity results (in particular, the dependence on n) may be disheartening, several improvements to the algorithm make it a practical tool in certain situations; we mention these below. Efficient methods for performing the tasks mentioned in the proof of Theorem 4.8 are detailed in [13]. Barvinok's algorithm has been implemented in computer software by at least two groups, resulting in LattE [12] and Barvinok 0.27 [31].
3) Recently, Köppe's primal irrational Barvinok algorithm has been implemented in LattE macchiato [24], providing speedups of "large factors" [25]. Irrational decompositions, introduced by Beck and Sottile [7], employ a shift vector so that the shift of a simple rational cone has the same integer points but contains no integer points on its proper faces. This strategy avoids inclusion-exclusion entirely.
4) Köppe's work also gives the option of stopped decompositions. This allows one to specify an integer l and terminate the decomposition procedure in the proof of Theorem 4.8 when all simple rational cones C_{ij} in (9) are of index at most l (rather than being of index 1, i.e., unimodular). The integer points in the associated fundamental parallepipeds of simple rational cones are then enumerated via Smith normal forms [25]. This may avoid what is often considered the bottleneck of Barvinok's algorithm.

Presently, the computational limitations of this approach arise from the size of the triangluations, specifically the number of cones in the triangluation and the indices of those cones. Available software can handle general cones in dimensions up to say 35, meaning $n + r \leq 35$. However, one may analyze particular codes in say dimension 50 or higher more easily than some codes of lower dimension due to their structure. More relevant than dimension (or code length) is the size of the triangulation involved. We hope that by providing this framework, we can identify codes which are easier to analyze and use this to shed light on more general situations.

As Barvinok's algorithm and integer point enumeration are relevant to a wide range of applications, it is reasonable to expect further refinements to available computational tools (and perhaps new ones). Problems currently out of reach may be reasonable in the near future. Thus, it is relevant to provide this framework for the study of pseudocodewords.

B. Irreducible Pseudocodewords

Recall that a nonzero pseudocodeword is irreducible if and only if it cannot be written as a sum of two or more nonzero pseudocodewords. Proposition 3.3 relates irreducible pseudocodewords to the Hilbert basis of the lifted fundamental cone via the projection π. In this subsection, we apply an element of the Barvinok-Woods projection algorithm to find the generating function for the irreducible pseudocodewords of a general parity-check code.

Definition 4.10: Given $H \in \mathbb{F}_2^{r \times n}$, the t-value of the Tanner graph of H, denoted t, is the maximum value that a coordinate of an irreducible pseudocodeword of $C(H)$ can have; that is

$$t := \max\{p_i : \mathbf{p} \in \mathrm{Irr}(H)\}.$$

According to Proposition 3.3, the set of irreducible pseudocodewords of $C(H)$ is finite as the Hilbert basis of K is finite [15]. It follows that the generating function of the irreducible pseudocodewords is always a rational function; in fact, it is a polynomial. Even so, producing such a polynomial directly is tantamount to listing all irreducible pseudocodewords. The following two results from Barvinok and Woods [5] yield a rational form for this polynomial without explicitly enumerating all the irreducible pseudocodewords. The first result concerns the projection of integer points of a rational polytope. The second result enables one to obtain the generating function for a set $S_1 \backslash S_2$ from the generating functions of finite sets S_1 and S_2 of integer vectors; of course, this is only of interest when $S_1 \cap S_2 \neq \emptyset$.

Lemma 4.11: ([5, Theorem 1.7]) Fix d. There exists a number $s = s(d)$ and a polynomial time algorithm which, given a rational polytope $P \subseteq \mathbb{R}^d$ and a linear transformation

$$T : \mathbb{R}^d \to \mathbb{R}^k$$

such that $T(\mathbb{Z}^d) \subseteq \mathbb{Z}^k$, expresses the generating function for $T(P \cap \mathbb{Z}^d)$ as

$$\sum_{i \in I} \alpha_i \frac{\mathbf{x}^{\mathbf{a}_i}}{(1 - \mathbf{x}^{\mathbf{u}_{i1}}) \cdots (1 - \mathbf{x}^{\mathbf{u}_{is}})}$$

where $\alpha_i \in \mathbb{Q}$ and $\mathbf{a}_i, \mathbf{u}_{ij}$ are integer vectors for all i, j.

Lemma 4.12: ([5, Corollary 3.7]) Fix s. Let $S_1, S_2 \subseteq \mathbb{Z}^d$ be finite sets. There exists a polynomial time algorithm which, given the generating functions for S_1 and S_2 in the form

$$\sum_{\mathbf{m} \in S_1} \mathbf{x}^{\mathbf{m}} = \sum_{i \in I_1} \alpha_i \frac{\mathbf{x}^{\mathbf{a}_i}}{(1 - \mathbf{x}^{\mathbf{u}_{i1}}) \cdots (1 - \mathbf{x}^{\mathbf{u}_{is}})}$$

and

$$\sum_{\mathbf{m} \in S_2} \mathbf{x}^{\mathbf{m}} = \sum_{i \in I_2} \beta_i \frac{\mathbf{x}^{\mathbf{b}_i}}{(1 - \mathbf{x}^{\mathbf{w}_{i1}}) \cdots (1 - \mathbf{x}^{\mathbf{w}_{is}})}$$

where $\alpha_i, \beta_i \in \mathbb{Q}$ and $\mathbf{a}_i, \mathbf{b}_i, \mathbf{u}_{ij}, \mathbf{w}_{ij}$ are integer vectors for all i, j, expresses the generating function for $S_1 \backslash S_2$ as

$$\sum_{\mathbf{m} \in S_1 \backslash S_2} \mathbf{x}^{\mathbf{m}} = \sum_{i \in I} \gamma_i \frac{\mathbf{x}^{\mathbf{c}_i}}{(1 - \mathbf{x}^{\mathbf{v}_{i1}}) \cdots (1 - \mathbf{x}^{\mathbf{v}_{is'}})}$$

where $s' \leq 2s$, $\gamma_i \in \mathbb{Q}$, and $\mathbf{c}_i, \mathbf{v}_{ij}$ are integer vectors for all i, j.

Theorem 4.13: Fix $d := n + r$. Given $H \in \mathbb{F}_2^{r \times n}$, there exists a polynomial time algorithm which computes the generating function of the irreducible pseudocodewords, $\sum_{\mathbf{p} \in \mathrm{Irr}(H)} \mathbf{x}^{\mathbf{p}}$, as a rational function.

Proof: We apply a technique similar to [5, Theorem 7.1]. Let

$$P = \left\{ (\mathbf{v}, \mathbf{a}) \in \mathbb{R}^d \;\middle|\; \begin{array}{l} v_i \geq 0, H\mathbf{v}^T = 2\mathbf{a}^T, \\ \sum_{l=1}^{n} h_{jl} v_l \geq 2h_{ji} v_i \\ \forall 1 \leq i \leq n, 1 \leq j \leq r, \\ 1 \leq \sum_{l=1}^{n} v_l, \text{and} \\ v_i \leq t \; \forall 1 \leq i \leq n \end{array} \right\}$$

where t is the t-value of the Tanner graph of H. Note that the set $\pi(P \cap \mathbb{Z}^{n+r})$ contains all the irreducible pseudocodewords of $C(H)$ where π is the projection defined in (1). Consider the map

$$\begin{array}{rccc} T: & P \times P & \to & \mathbb{R}^n \\ & ((\mathbf{v}_1, \mathbf{a}_1), (\mathbf{v}_2, \mathbf{a}_2)) & \mapsto & \mathbf{v}_1 + \mathbf{v}_2. \end{array}$$

Let

$$L_1 = \pi(P \cap \mathbb{Z}^d)$$

and

$$L_2 = T((P \times P) \cap \mathbb{Z}^{2d}).$$

We claim that the set of irreducible pseudocodewords of $C(H)$ is given by

$$\mathrm{Irr}(H) = L_1 \backslash L_2.$$

To prove the claim, first note that $L_1, L_2 \subseteq \mathsf{PC}(H)$ by Proposition 3.2. Let $\mathbf{p} \in \mathrm{Irr}(H)$ be an irreducible pseudocodeword of $C(H)$. Then $\mathbf{p} \in L_1$ by the construction of P. However, $\mathbf{p} \notin L_2$ since $\mathbf{p}$ cannot be written as a sum of two or more nonzero pseudocodewords. Therefore, $\mathbf{p} \in L_1 \backslash L_2$. Hence

$$\mathrm{Irr}(H) \subseteq L_1 \backslash L_2.$$

Now consider $\mathbf{p} \in L_1 \backslash L_2$. According to Proposition 3.2, $\mathbf{p}$ is a pseudocodeword of $C(H)$. Suppose

$$\mathbf{p} = \mathbf{y}_1 + \mathbf{y}_2$$

where $\mathbf{y}_1$ and $\mathbf{y}_2$ are nonzero pseudocodewords. It follows that $p_i \geq y_{1i}, y_{2i}$. By Proposition 3.2,

$$\mathbf{p} = \pi(\mathbf{p}, \mathbf{a}),$$
$$\mathbf{y}_1 = \pi(\mathbf{y}_1, \mathbf{a}_1),$$
and
$$\mathbf{y}_2 = \pi(\mathbf{y}_2, \mathbf{a}_2),$$

for some $(\mathbf{p}, \mathbf{a}), (\mathbf{y}_1, \mathbf{a}_1), (\mathbf{y}_2, \mathbf{a}_2) \in \hat{\mathcal{K}}(H)$. Since $\mathbf{p} \in L_1$, $(\mathbf{p}, \mathbf{a}) \in P$. This implies $(\mathbf{y}_1, \mathbf{a}_1), (\mathbf{y}_2, \mathbf{a}_2) \in P$. It follows that

$$\mathbf{p} = T((\mathbf{y}_1, \mathbf{a}_1), (\mathbf{y}_2, \mathbf{a}_2)) \in L_2,$$

contradicting the assumption that $\mathbf{p} \in L_1 \backslash L_2$. Therefore, $\mathbf{p}$ is irreducible. This proves the claim.

Applying Lemma 4.11 to L_1 and L_2 gives rational forms for the generating functions of L_1 and L_2. If necessary, these expressions may be manipulated, multiplying terms by expressions of the form $\frac{1 - \mathbf{x}^{\mathbf{u}_{ij}}}{1 - \mathbf{x}^{\mathbf{u}_{ij}}}$ as needed, so that s as in Lemma 4.12 is obtained. Finally, an application of Lemma 4.12 to determine $\sum_{\mathbf{m} \in L_1 \backslash L_2} \mathbf{x}^{\mathbf{m}}$ completes the proof as

$$\sum_{\mathbf{p} \in \mathrm{Irr}(H)} \mathbf{x}^{\mathbf{p}} = \sum_{\mathbf{m} \in L_1 \backslash L_2} \mathbf{x}^{\mathbf{m}}.$$

■

Remark 4.14: Similar to Lemma 4.7, the complexity of Lemmas 4.11 and 4.12 is polynomial with respect to number of bits needed to describe the input assuming the dimension is fixed. In Lemma 4.11, the input size of the linear transformation T is $\sum_{i,j} \chi(t_{ij})$; the input size of the polytope P defined by rational inequalities $\mathbf{c}_i^T \mathbf{x} \leq \beta_i$, $i = 1, \ldots, n$, is

$$\sum_{i=1}^{n} \chi(\beta_i) + \sum_{i=1}^{n} \sum_{j=1}^{d} \chi(c_{ij}).$$

The input size in Lemma 4.12 is the input size of the rational forms of the generating functions of S_1 and S_2, each of which is found as in (4).

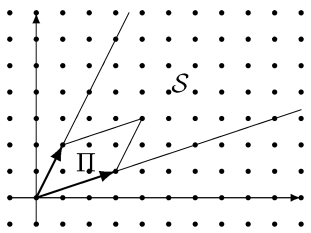
While the Barvinok-Woods algorithm may be a promising tool for studying the set of irreducible pseudocodewords, the algorithm involves complicated routines such as algorithmic flat-

ness theory and iterated Boolean combinations of rational generating functions; we do not know of any implementation of the algorithm in the literature. Enumerating the irreducible pseudocodewords (and the Hilbert basis in general) remains a generally hard task. Nevertheless, the Hilbert basis can be efficiently computed in some circumstances. A project-and-lift algorithm by Hemmecke [16] has been implemented in the software 4ti2 [17].

V. Examples

This section contains examples illustrating the ideas in Section IV.

Example 5.1: Let $\mathbf{u}_1 = (3,1), \mathbf{u}_2 = (1,2) \in \mathbb{Z}^2$. Then the simple rational cone $\mathcal{S}$ and the fundamental parallelepiped Π generated by $\mathbf{u}_1$ and $\mathbf{u}_2$ are as shown below.



Then

$$\sum_{\mathbf{m}\in\mathcal{S}\cap\mathbb{Z}^2} \mathbf{x}^{\mathbf{m}} = \left(\sum_{\mathbf{m}\in\Pi\cap\mathbb{Z}^2} \mathbf{x}^{\mathbf{m}}\right) \prod_{i=1}^{2} \frac{1}{1-\mathbf{x}^{\mathbf{u}_i}} = \frac{1+x_1x_2+x_1^2x_2+x_1^2x_2^2+x_1^3x_2^2}{(1-x_1^3x_2)\,(1-x_1x_2^2)}.$$

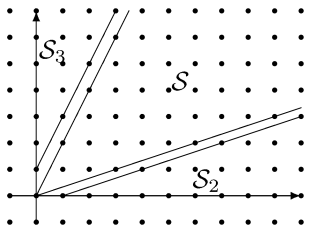
Barvinok 0.27 computes the generating function of the integer points in $\mathcal{S}$ to be

$$\sum_{\mathbf{m}\in\mathcal{S}\cap\mathbb{Z}^2} \mathbf{x}^{\mathbf{m}} = \frac{1}{(1-x_1)(1-x_2)} - \frac{x_1}{(1-x_1)\,(1-x_1^3x_2)} - \frac{x_2}{(1-x_2)\,(1-x_1x_2^2)}.$$

The above rational form results from noting that the integer points in $\mathcal{S}$ are the same as those in

$$\mathcal{S}_1 \backslash (\mathcal{S}_2 \cup S_3)$$

where $\mathcal{S}_1$ is the first quadrant, $\mathcal{S}_2$ is the rational cone generated by (1, 0) and (3, 1) with a vertex at (1, 0), and $\mathcal{S}_3$ is the rational cone generated by (0, 1) and (1, 2) with a vertex at (0, 1) as shown below.



Here, one may note that $\mathcal{S}_1$, $\mathcal{S}_2$, and $\mathcal{S}_3$ are all shifts of unimodular cones.

Example 5.2: Consider the code $C(H)$ given by parity-check matrix

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

Barvinok 0.27 computes

$$\sum_{\mathbf{p}\in\mathsf{PC}(H)} \mathbf{x}^{\mathbf{p}} = \frac{1}{(1-x_1x_2x_3)(1-x_1x_2x_3x_4^2x_5x_6x_7)(1-x_5x_6x_7)}.$$

It is interesting to see that the above rational form for $\sum_{\mathbf{p}\in\mathsf{PC}(H)} \mathbf{x}^{\mathbf{p}}$ implies that

$$(1,1,1,0,0,0,0),$$
$$(1,1,1,2,1,1,1),$$
$$\text{and}$$
$$(0,0,0,0,1,1,1)$$

are the only irreducible pseudocodewords of $C(H)$.

The code $C(H)$ is also studied in [21], [22] where the edge zeta function of the normal graph of $C(H)$ is found. While the rational form of the generating function above is simpler than that of [21], [22], it lacks the combinatorial connection of the edge zeta function.

Example 5.3: In this example, we consider the $[7,3,4]$ simplex code with two different choices for parity-check matrix. Let

$$H_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$
$$\text{and}$$
$$H_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Note that H_1 and H_2 differ only in the last row. The last row of H_2 is the binary sum of the last two rows of H_1.

The irreducible pseudocodewords of $C(H_1)$ and $C(H_2)$ are found using 4ti2 [17]. The irreducible pseudocodewords of $C(H_1)$ which are not codewords of $C(H_1)$ are the following:

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

Since the parity-check matrices H_1 and H_2 are nearly identical, one may expect the pseudocodewords of $C(H_2)$ and the pseudocodewords of $C(H_1)$ to be mostly the same. On the contrary, while there are only 20 irreducible pseudocodewords for $C(H_1)$, 4ti2 finds 39 irreducible pseudocodewords for $C(H_2)$. Moreover

$$\mathrm{Irr}(H_1) \subsetneqq \mathrm{Irr}(H_2).$$

This implies

$$K(H_1) \subsetneqq K(H_2).$$

One may infer that the $[7, 3, 4]$ simplex code represented by H_2 is more prone to error than the same code represented by H_1.

It is interesting to note that the irreducible pseudocodewords of $C(H_1)$ coincide with the minimal pseudocodewords of $C(H_1)$ found in [28].

The choice of the parity-check matrix is important to message-passing iterative and LP decoders, and to better understand this we need information on the pseudocodewords. While several of the algorithms mentioned have been implemented in software, there are still limitations to the size of the problem the software can handle. Even so, new approaches are resulting in great speed-ups. For now, it may be the case that some of the ideas described here provide theoretical tools for the study of pseudocodewords and code representation. Perhaps these will be helpful in making a more combinatorial connection between the generating function of the pseudocodewords and a graphical representation of the code, as in the cycle code case.

VI. Conclusion

In this paper, we introduce the lifted fundamental cone as a tool for studying the pseudocodewords of a binary linear code. The approach taken here yields a rational function that enumerates the pseudocodewords of a general parity-check code and provides new tools to aid in the study of pseudocodewords (and irreducible pseudocodewords). Applying Barvinok's algorithm to the lifted fundamental cone yields a polynomial time algorithm for producing the generating function for the pseudocodewords. Moreover, the set of irreducible pseudocodewords is simply a projection of the Hilbert basis for the cone. This makes it possible to use computational tools and their software implementations to study the pseudocodewords of a parity-check code.

Acknowledgment

The authors would like to thank the reviewers for their helpful comments and suggestions, as well as R. Hemmecke and M. Köppe for their useful insights.

References

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

[2] A. Barvinok, "A polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed," *Math. Oper. Res.*, vol. 19, no. 4, pp. 769–779, 1994.

[3] A. Barvinok, Amer. Math. Soc., Providence, RI, "Lattice points, polyhedra, and complexity, geometric combinatorics, 19–62," *IAS/Park City Math.*, ser. 13, 2007.

[4] A. Barvinok and J. Pommersheim, "An algorithmic theory of lattice points in polyhedra, new perspectives in algebraic combinatorics (Berkeley, CA, 1996–97," in *Math. Sci. Res. Inst. Publ.*. Cambridge, U.K.: Cambridge Univ. Press, 1999, vol. 38, pp. 91–147.

[5] A. Barvinok and K. Woods, "Short rational generating functions for lattice point problems," *J. Amer. Math. Soc.*, vol. 16, no. 4, pp. 957–979, 2003.

[6] M. Beck and S. Robins, *Computing the Continuous Discretely: Integer-Point Enumeration in Polyhedra*. New York: Springer, 2007.

[7] M. Beck and F. Sottile, "Irrational proofs for three theorems of Stanley," *Eur. J. Combin.*, vol. 28, no. 1, pp. 403–409, 2007.

[8] M. Breitbach, M. Bossert, R. Lucas, and C. Kempter, "Letter soft-decision decoding of linear block codes as optimization problem," *Eur. Trans. Telecommun.*, vol. 9, no. 3, pp. 289–293, 1998.

[9] M. Brion, "Points entiers dans les polyèdres convexes," (in French) *Ann. Sci. École Norm. Sup. (4)*, vol. 21, no. 4, pp. 653–663, 1988, [Lattice points in convex polyhedra].

[10] T. D. Coleman, Pseudocodewords Presentation Cambridge, MA, MIT Tech. Rep., 2003.

[11] J. G. van der Corput, "Uber Systeme von linear-homogenen Gleichungen und Ungleichungen," in *Proc. Koninklijke Akademie van Wetenschappen te Amsterdam*, 1931, vol. 34, pp. 368–371.

[12] J. A. De Loera, D. Haws, R. Hemmecke, P. Huggins, J. Tauzer, and R. Yoshida, "A user's guide for LattE v1.1," 2003, software package LattE is available at [Online]. Available: http://www.math.ucdavis.edu/~latte/

[13] J. A. De Loera, R. Hemmecke, J. Tauzer, and R. Yoshida, "Effective lattice point counting in rational convex polytopes," *J. Symbol. Comput.*, vol. 38, no. 4, pp. 1273–1302, 2004.

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

[15] P. Gordan, "Über die Auflösung linearer Gleichungen mit reellen Coefficienten," *Math. Ann.*, vol. 6, no. 1, pp. 23–28, 1873.

[16] R. Hemmecke, "On the computation of Hilbert bases of cones," in *Proc. 1st Int. Congr. Mathematical Software*, Beijing, China, 2002.

[17] R. Hemmecke, M. Köppe, P. Malkin, and M. Walter, "4ti2—A software package for algebraic, geometric and combinatorial problems on linear spaces," [Online]. Available: http://www.4ti2.de

[18] M. Henk and R. Weismantel, "On Hilbert bases of polyhedral cones," *Results in Math.*, vol. 32, pp. 298–303, 1997.

[19] R. Kannan, "Lattice translates of a polytope and the Frobenius problem," *Combinatorica*, vol. 12, pp. 161–177, 1992.

[20] C. Kelley and D. Sridhara, "Pseudocodewords of Tanner graphs," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 4013–4038, Nov. 2007.

[21] R. Koetter, W.-C. W. Li, P. O. Vontobel, and J. Walker, "Pseudo-codewords of cycle codes via zeta functions," in *Proc. IEEE Information Theory Workshop*, San Antonio, TX, 2004, pp. 7–12, IEEE.

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

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

[24] M. Köppe, LattE Macchiato Version 1.2-mk-0.9.3, available at [Online]. Available: http://www.math.ucdavis.edu/~mkoeppe

[25] M. Köppe, "A primal Barvinok algorithm based on irrational decompositions," *SIAM J. Discrete Math.*, vol. 21, no. 1, pp. 220–236, 2007.

[26] M. Köppe, S. Verdoolaege, and K. Woods, "An implementation of the Barvinok-Woods integer projection algorithm," in *Proc. Int. Conf. Information Theory and Stat. Learning*, 2008, pp. 53–59.

[27] W.-C. W. Li, M. Lu, and C. Wang, "Recent developments in low-density parity-check codes," *Lecture Notes in Comput. Sci.*, vol. 5557, pp. 107–123, 2009.

[28] R. Smarandache and P. O. Vontobel, "Pseudo-codeword analysis of Tanner graphs from projective and Euclidean planes," *IEEE Trans. Inf. Theory*, vol. 53, no. 7, pp. 2376–2393, Jul. 2007.

[29] R. P. Stanley, *Enumerative Combinatorics, Vol. 1, Corrected Reprint of the 1986 Original, Cambridge Studies in Advanced Mathematics*. Cambridge, U.K.: Cambridge Univ. Press, 1997, vol. 49.

[30] R. M. Tanner, "A recursive approach to low-complexity codes," *IEEE Trans. Inf. Theory*, vol. IT-27, no. 5, pp. 533–547, Sep. 1981.

[31] S. Verdoolaege, K. Woods, M. Bruynooghe, and R. Cools, Computation and Manipulation of Enumerators of Integer Projections of Parametric Polytopes CW Report, 2005, vol. CW392 [Online]. Available: http://www.kotnet.org/~skimo/barvinok/

[32] P. O. Vontobel, "Connecting the Bethe entropy and the edge zeta function of a cycle code," in *Proc. IEEE Int. Symp. Information Theory*, Austin, TX, Jun. 13–18, 2010, pp. 704–708.
[33] P. O. Vontobel and R. Koetter, "Graph-cover decoding and finite-length analysis of message-passing iterative decoding of LDPC codes," *IEEE Trans. Inf. Theory*, to be published.

Wittawat Kositwattanarerk received the B.A. degrees in mathematics and economics from the University of Virginia, Charlottesville, in 2006. He is currently pursuing the Ph.D. degree in mathemetical sciences at Clemson University, Clemson, SC.

His research interests are in algebraic coding theory, including error control coding and belief propagation on graphs.

Gretchen L. Matthews received the B.S. degree in mathematics from Oklahoma State University, Oklahoma City, in 1995 and the Ph.D. degree in mathematics from Louisiana State University, Baton Rouge, in 1999.

Following postdoctoral work at the University of Tennessee, she joined the faculty in the Department of Mathematical Sciences, Clemson University, Clemson, SC, where she is currently an Associate Professor. Her research interests include algebra and its applications.