Polytope Representations for Linear-Programming Decoding of Non-Binary Linear Codes

Vitaly Skachek
Claude Shannon Institute
University College Dublin
Belfield, Dublin 4, Ireland
vitaly.skachek@ucd.ie

Mark F. Flanagan
DEIS
University of Bologna
47023 Cesena, Italy
mark.flanagan@ieee.org

Eimear Byrne[1]
School of Mathematical Sciences
University College Dublin
Belfield, Dublin 4, Ireland
ebyrne@ucd.ie

Marcus Greferath[1]
School of Mathematical Sciences
University College Dublin
Belfield, Dublin 4, Ireland
marcus.greferath@ucd.ie

***Abstract*— In previous work, we demonstrated how decoding of a non-binary linear code could be formulated as a linear-programming problem. In this paper, we study different polytopes for use with linear-programming decoding, and show that for many classes of codes these polytopes yield a complexity advantage for decoding. These representations lead to polynomial-time decoders for a wide variety of classical non-binary linear codes.**

I. Introduction

In [1] and [2], the decoding of *binary* LDPC codes using linear-programming decoding was proposed, and the connections between linear-programming decoding and classical belief propagation decoding were established. In [3], the approach of [2] was extended to coded modulation, in particular to codes over rings mapped to non-binary modulation signals. In both cases, the principal advantage of the linear-programming framework is its mathematical tractability [2], [3].

For the binary coding framework, alternative polytope representations were studied which gave a complexity advantage in certain scenarios [1], [2], [4], [5]. Analagous to the work of [1], [2], [4], [5] for binary codes, we define two polytope representations alternative to that proposed in [3] which offer a smaller number of variables and constraints for many classes of nonbinary codes. We compare these representations with the polytope in [3]. These representations are also shown to have equal error-correcting performance to the polytope in [3].

II. Linear-programming Decoding

Consider codes over finite quasi-Frobenius rings (this includes codes over finite fields, but may be more general). Denote by $\mathfrak{R}$ such a ring with q elements, by 0 its additive identity, and let $\mathfrak{R}^- = \mathfrak{R}\backslash\{0\}$. Let $\mathcal{C}$ be a linear code of length n over $\mathfrak{R}$ with $m \times n$ parity-check matrix $\mathcal{H}$.

Denote the set of column indices and the set of row indices of $\mathcal{H}$ by $\mathcal{I} = \{1, 2, \cdots, n\}$ and $\mathcal{J} = \{1, 2, \cdots, m\}$, respectively. The notation $\mathcal{H}_j$ will be used for the j-th row of $\mathcal{H}$. Denote by $\text{supp}(\boldsymbol{c})$ the support of a vector $\boldsymbol{c}$. For each $j \in \mathcal{J}$, let $\mathcal{I}_j = \text{supp}(\mathcal{H}_j)$ and $d_j = |\mathcal{I}_j|$, and let $d = \max_{j \in \mathcal{J}}\{d_j\}$.

[1]These authors are also affiliated with the Claude Shannon Institute for Discrete Mathematics, Coding and Cryptography.

Given any $\boldsymbol{c} \in \mathfrak{R}^n$, parity check $j \in \mathcal{J}$ is *satisfied* by $\boldsymbol{c}$ if and only if the following equality holds over $\mathfrak{R}$:

$$\sum_{i \in \mathcal{I}_j} c_i \cdot \mathcal{H}_{j,i} = 0 \; . \quad (1)$$

For $j \in \mathcal{J}$, define the single parity check code $\mathcal{C}_j$ by

$$\mathcal{C}_j = \{(b_i)_{i \in \mathcal{I}_j} \; : \; \sum_{i \in \mathcal{I}_j} b_i \cdot \mathcal{H}_{j,i} = 0\}$$

Note that while the symbols of the codewords in $\mathcal{C}$ are indexed by $\mathcal{I}$, the symbols of the codewords in $\mathcal{C}_j$ are indexed by $\mathcal{I}_j$. Observe that $\boldsymbol{c} \in \mathcal{C}$ if and only if all parity checks $j \in \mathcal{J}$ are satisfied by $\boldsymbol{c}$.

Assume that the codeword $\bar{\boldsymbol{c}} = (\bar{c}_1, \bar{c}_2, \cdots, \bar{c}_n) \in \mathcal{C}$ has been transmitted over a q-ary input memoryless channel, and a corrupted word $\boldsymbol{y} = (y_1, y_2, \cdots, y_n) \in \Sigma^n$ has been received. Here Σ denotes the set of channel output symbols. In addition, assume that all codewords are transmitted with equal probability.

For vectors $\boldsymbol{f} \in \mathbb{R}^{(q-1)n}$, the notation

$$\boldsymbol{f} = (\boldsymbol{f}_1 \mid \boldsymbol{f}_2 \mid \; \cdots \; \mid \boldsymbol{f}_n) \; ,$$

will be used, where

$$\forall i \in \mathcal{I}, \; \boldsymbol{f}_i = (f_i^{(\alpha)})_{\alpha \in \mathfrak{R}^-} \; .$$

We also define a function $\boldsymbol{\lambda} : \Sigma \longrightarrow (\mathbb{R} \cup \{\pm\infty\})^{q-1}$ by

$$\boldsymbol{\lambda} = (\lambda^{(\alpha)})_{\alpha \in \mathfrak{R}^-} \; ,$$

where, for each $y \in \Sigma$, $\alpha \in \mathfrak{R}^-$,

$$\lambda^{(\alpha)}(y) = \log\left(\frac{p(y|0)}{p(y|\alpha)}\right) \; ,$$

and $p(y|c)$ denotes the channel output probability (density) conditioned on the channel input. Extend $\boldsymbol{\lambda}$ to a map on Σ^n by $\boldsymbol{\lambda}(\boldsymbol{y}) = (\boldsymbol{\lambda}(y_1) \mid \boldsymbol{\lambda}(y_2) \mid \; \ldots \; \mid \boldsymbol{\lambda}(y_n))$.

The LP decoder in [3] performs the following cost function minimization:

$$(\hat{\boldsymbol{f}}, \hat{\boldsymbol{w}}) = \arg \min_{(\boldsymbol{f}, \boldsymbol{w}) \in \mathcal{Q}} \boldsymbol{\lambda}(\boldsymbol{y}) \boldsymbol{f}^T \; , \quad (2)$$

where the polytope $\mathcal{Q}$ is a relaxation of the convex hull of all points $\boldsymbol{f} \in \mathbb{R}^{(q-1)n}$, which correspond to codewords; this polytope is defined as the set of $\boldsymbol{f} \in \mathbb{R}^{(q-1)n}$, together with the auxiliary variables

$$w_{j,\boldsymbol{b}} \text{ for } j \in \mathcal{J}, \boldsymbol{b} \in \mathcal{C}_j \ ,$$

which satisfy the following constraints:

$$\forall j \in \mathcal{J}, \ \forall \boldsymbol{b} \in \mathcal{C}_j, \quad w_{j,\boldsymbol{b}} \geq 0 \ , \tag{3}$$

$$\forall j \in \mathcal{J}, \quad \sum_{\boldsymbol{b} \in \mathcal{C}_j} w_{j,\boldsymbol{b}} = 1 \ , \tag{4}$$

and

$$\forall j \in \mathcal{J}, \ \forall i \in \mathcal{I}_j, \ \forall \alpha \in \mathfrak{R}^-, \quad f_i^{(\alpha)} = \textstyle\sum_{\boldsymbol{b} \in \mathcal{C}_j, \ b_i = \alpha} w_{j,\boldsymbol{b}} \ . \tag{5}$$

The minimization of the objective function (2) over $\mathcal{Q}$ forms the relaxed LP decoding problem. The number of variables and constraints for this LP are upper-bounded by $n(q-1)+mq^{d-1}$ and $m(q^{d-1}+d(q-1)+1)$ respectively.

It is shown in [3] that if $\hat{\boldsymbol{f}}$ is integral, the decoder output corresponds to the maximum-likelihood (ML) codeword. Otherwise, the decoder outputs an 'error'.

III. New LP Description

The results in this section are a generalization of the high-density polytope representation [2, Appendix II]. Recall that the ring $\mathfrak{R}$ contains $q-1$ non-zero elements. Correspondingly, for vectors $\boldsymbol{k} \in \mathbb{N}^{q-1}$, we adopt the notation

$$\boldsymbol{k} = (k_\alpha)_{\alpha \in \mathfrak{R}^-}$$

Now, for any $j \in \mathcal{J}$, we define the mapping

$$\begin{array}{rccl} \boldsymbol{\kappa}_j \ : \ \mathcal{C}_j & \longrightarrow & \mathbb{N}^{q-1} \ , \\ \boldsymbol{b} & \mapsto & \boldsymbol{\kappa}_j(\boldsymbol{b}) \end{array}$$

defined by

$$(\boldsymbol{\kappa}_j(\boldsymbol{b}))_\alpha = |\{ i \in \mathcal{I}_j \ : \ b_i \cdot \mathcal{H}_{j,i} = \alpha \}|$$

for all $\alpha \in \mathfrak{R}^-$. We may then characterize the image of $\boldsymbol{\kappa}_j$, which we denote by $\mathcal{T}_j$, as

$$\mathcal{T}_j = \left\{ \boldsymbol{k} \in \mathbb{N}^{q-1} \ : \ \sum_{\alpha \in \mathfrak{R}^-} \alpha \cdot k_\alpha = 0 \text{ and } \sum_{\alpha \in \mathfrak{R}^-} k_\alpha \leq d_j \right\} \ ,$$

for each $j \in \mathcal{J}$, where, for any $k \in \mathbb{N}$, $\alpha \in \mathfrak{R}$,

$$\alpha \cdot k = \begin{cases} 0 & \text{if } k = 0 \\ \alpha + \cdots + \alpha & \text{if } k > 0 \ (k \text{ terms in sum}) \end{cases} \ .$$

The set $\mathcal{T}_j$ is equal to the set of all possible vectors $\boldsymbol{\kappa}_j(\boldsymbol{b})$ for $\boldsymbol{b} \in \mathcal{C}_j$.

Note that $\boldsymbol{\kappa}_j$ is not a bijection, in general. We say that a local codeword $\boldsymbol{b} \in \mathcal{C}_j$ is $\boldsymbol{k}$-constrained over $\mathcal{C}_j$ if $\boldsymbol{\kappa}_j(\boldsymbol{b}) = \boldsymbol{k}$.

Next, for any index set $\Gamma \subseteq \mathcal{I}$, we introduce the following definitions. Let $N = |\Gamma|$. We define the single-parity-check-code, over vectors indexed by Γ, by

$$\mathcal{C}_\Gamma = \left\{ \boldsymbol{a} = (a_i)_{i \in \Gamma} \in \mathfrak{R}^N \ : \ \sum_{i \in \Gamma} a_i = 0 \right\} \ . \tag{6}$$

Also define a mapping $\boldsymbol{\kappa}_\Gamma \ : \ \mathcal{C}_\Gamma \longrightarrow \mathbb{N}^{q-1}$ by

$$(\boldsymbol{\kappa}_\Gamma(\boldsymbol{a}))_\alpha = |\{ i \in \Gamma \ : \ a_i = \alpha \}| \ ,$$

and define, for $\boldsymbol{k} \in \mathcal{T}_j$,

$$\mathcal{C}_\Gamma^{(\boldsymbol{k})} = \{ \boldsymbol{a} \in \mathcal{C}_\Gamma \ : \ \boldsymbol{\kappa}_\Gamma(\boldsymbol{a}) = \boldsymbol{k} \} \ .$$

Below, we define a new polytope for decoding. Recall that $\boldsymbol{y} = (y_1, y_2, \cdots, y_n) \in \Sigma^n$ stands for the received (corrupted) word. In the sequel, we make use of the following variables:

- For all $i \in \mathcal{I}$ and all $\alpha \in \mathfrak{R}^-$, we have a variable $f_i^{(\alpha)}$. This variable is an indicator of the event $y_i = \alpha$.
- For all $j \in \mathcal{J}$ and $\boldsymbol{k} \in \mathcal{T}_j$, we have a variable $\sigma_{j,\boldsymbol{k}}$. Similarly to its counterpart in [2], this variable indicates the contribution to parity check j of $\boldsymbol{k}$-constrained local codewords over $\mathcal{C}_j$.
- For all $j \in \mathcal{J}$, $i \in \mathcal{I}_j$, $\boldsymbol{k} \in \mathcal{T}_j$, $\alpha \in \mathfrak{R}^-$, we have a variable $z_{i,j,\boldsymbol{k}}^{(\alpha)}$. This variable indicates the portion of $f_i^{(\alpha)}$ assigned to $\boldsymbol{k}$-constrained local codewords over $\mathcal{C}_j$.

Motivated by these variable definitions, for all $j \in \mathcal{J}$ we impose the following set of constraints:

$$\forall i \in \mathcal{I}_j, \forall \alpha \in \mathfrak{R}^-, \qquad f_i^{(\alpha)} = \sum_{\boldsymbol{k} \in \mathcal{T}_j} z_{i,j,\boldsymbol{k}}^{(\alpha)} \ . \tag{7}$$

$$\sum_{\boldsymbol{k} \in \mathcal{T}_j} \sigma_{j,\boldsymbol{k}} = 1 \ . \tag{8}$$

$$\forall \boldsymbol{k} \in \mathcal{T}_j, \forall \alpha \in \mathfrak{R}^-, \quad \sum_{i \in \mathcal{I}_j, \ \beta \in \mathfrak{R}^-, \ \beta \mathcal{H}_{j,i} = \alpha} z_{i,j,\boldsymbol{k}}^{(\beta)} = k_\alpha \cdot \sigma_{j,\boldsymbol{k}} \ . \tag{9}$$

$$\forall i \in \mathcal{I}_j, \forall \boldsymbol{k} \in \mathcal{T}_j, \forall \alpha \in \mathfrak{R}^-, \qquad z_{i,j,\boldsymbol{k}}^{(\alpha)} \geq 0 \ . \tag{10}$$

$$\forall i \in \mathcal{I}_j, \forall \boldsymbol{k} \in \mathcal{T}_j, \quad \sum_{\alpha \in \mathfrak{R}^-} \ \sum_{\beta \in \mathfrak{R}^-, \ \beta \mathcal{H}_{j,i} = \alpha} z_{i,j,\boldsymbol{k}}^{(\beta)} \leq \sigma_{j,\boldsymbol{k}} \ . \tag{11}$$

We note that the further constraints

$$\forall i \in \mathcal{I}, \forall \alpha \in \mathfrak{R}^-, \qquad 0 \leq f_i^{(\alpha)} \leq 1 \ , \tag{12}$$

$$\forall j \in \mathcal{J}, \forall \boldsymbol{k} \in \mathcal{T}_j, \qquad 0 \leq \sigma_{j,\boldsymbol{k}} \leq 1 \ , \tag{13}$$

and

$$\forall j \in \mathcal{J}, \forall i \in \mathcal{I}_j, \forall \boldsymbol{k} \in \mathcal{T}_j, \forall \alpha \in \mathfrak{R}^-, \quad z_{i,j,\boldsymbol{k}}^{(\alpha)} \leq \sigma_{j,\boldsymbol{k}} \ , \tag{14}$$

follow from constraints (7)-(11). We denote by $\mathcal{U}$ the polytope formed by constraints (7)-(11).

Let $T = \max_{j \in \mathcal{J}} |\mathcal{T}_j|$. Then, upper bounds on the number of variables and constraints in this LP are given by $n(q-1)+m(d(q-1)+1)T$ and $m(d(q-1)+1)+m((d+1)(q-1)+d)T$, respectively. Since $T \leq \binom{d+q-1}{d}$, the number of variables and constraints are $O(mq \cdot d^q)$, which, for many families of codes, is significantly lower than the corresponding complexity for polytope $\mathcal{Q}$.

For notational simplicity in proofs in this paper, it is convenient to define a new set of variables as follows:

$$\forall j \in \mathcal{J}, \forall i \in \mathcal{I}_j, \forall \boldsymbol{k} \in \mathcal{T}_j, \forall \alpha \in \Re^-, \quad \tau_{i,j,\boldsymbol{k}}^{(\alpha)} = \sum_{\beta \in \Re^-,\, \beta\mathcal{H}_{j,i} = \alpha} z_{i,j,\boldsymbol{k}}^{(\beta)} \,. \quad (15)$$

Then constraints (9) and (11) may be rewritten as

$$\forall j \in \mathcal{J}, \boldsymbol{k} \in \mathcal{T}_j, \forall \alpha \in \Re^-, \qquad \sum_{i \in \mathcal{I}_j} \tau_{i,j,\boldsymbol{k}}^{(\alpha)} = k_\alpha \cdot \sigma_{j,\boldsymbol{k}} \,, \quad (16)$$

$$\forall j \in \mathcal{J}, \forall i \in \mathcal{I}_j, \forall \boldsymbol{k} \in \mathcal{T}_j, \quad 0 \le \sum_{\alpha \in \Re^-} \tau_{i,j,\boldsymbol{k}}^{(\alpha)} \le \sigma_{j,\boldsymbol{k}} \,. \quad (17)$$

Note that the variables $\boldsymbol{\tau}$ do not form part of the LP description, and therefore do not contribute to its complexity. However these variables will provide a convenient notational shorthand for proving results in this paper.

We will prove that optimizing the cost function (2) over this new polytope is equivalent to optimizing over $\mathcal{Q}$. First, we state the following proposition, which will be necessary to prove this result.

Proposition 3.1: Let $M \in \mathbb{N}$ and $\boldsymbol{k} \in \mathbb{N}^{q-1}$. Also let $\Gamma \subseteq \mathcal{I}$. Assume that for each $\alpha \in \Re^-$, we have a set of nonnegative integers $\mathcal{X}^{(\alpha)} = \{x_i^{(\alpha)} \,:\, i \in \Gamma\}$ and that together these satisfy the constraints

$$\sum_{i \in \Gamma} x_i^{(\alpha)} = k_\alpha M \quad (18)$$

for all $\alpha \in \Re^-$, and

$$\sum_{\alpha \in \Re^-} x_i^{(\alpha)} \le M \quad (19)$$

for all $i \in \Gamma$.

Then, there exist nonnegative integers $\left\{ w_{\boldsymbol{a}} \,:\, \boldsymbol{a} \in \mathcal{C}_\Gamma^{(\boldsymbol{k})} \right\}$ such that

1) $$\sum_{\boldsymbol{a} \in \mathcal{C}_\Gamma^{(\boldsymbol{k})}} w_{\boldsymbol{a}} = M \,. \quad (20)$$

2) For all $\alpha \in \Re^-$, $i \in \Gamma$,
$$x_i^{(\alpha)} = \sum_{\boldsymbol{a} \in \mathcal{C}_\Gamma^{(\boldsymbol{k})},\, a_i = \alpha} w_{\boldsymbol{a}} \,. \quad (21)$$

A sketch of the proof of this proposition will follow at the end of this section. We now prove the main result.

Theorem 3.2: The set $\bar{\mathcal{U}} = \{\boldsymbol{f} : \exists\ \boldsymbol{\sigma}, \boldsymbol{z} \text{ s.t. } (\boldsymbol{f}, \boldsymbol{\sigma}, \boldsymbol{z}) \in \mathcal{U}\}$ is equal to the set $\bar{\mathcal{Q}} = \{\boldsymbol{f} : \exists\ \boldsymbol{w} \text{ s.t. } (\boldsymbol{f}, \boldsymbol{w}) \in \mathcal{Q}\}$. Therefore, optimizing the linear cost function (2) over $\mathcal{U}$ is equivalent to optimizing over $\mathcal{Q}$.

Proof:

1) Suppose, $(\boldsymbol{f}, \boldsymbol{w}) \in \mathcal{Q}$. For all $j \in \mathcal{J}, \boldsymbol{k} \in \mathcal{T}_j$, we define

$$\sigma_{j,\boldsymbol{k}} = \sum_{\boldsymbol{b} \in \mathcal{C}_j,\, \boldsymbol{\kappa}_j(\boldsymbol{b}) = \boldsymbol{k}} w_{j,\boldsymbol{b}} \,,$$

and for all $j \in \mathcal{J},\ i \in \mathcal{I}_j,\ \boldsymbol{k} \in \mathcal{T}_j,\ \alpha \in \Re^-$, we define

$$z_{i,j,\boldsymbol{k}}^{(\alpha)} = \sum_{\boldsymbol{b} \in \mathcal{C}_j,\, \boldsymbol{\kappa}_j(\boldsymbol{b}) = \boldsymbol{k},\, b_i = \alpha} w_{j,\boldsymbol{b}} \,,$$

It is straightforward to check that constraints (10) and (11) are satisfied by these definitions.
For every $j \in \mathcal{J},\ i \in \mathcal{I}_j,\ \alpha \in \Re^-$, we have by (5)

$$f_i^{(\alpha)} = \sum_{\boldsymbol{b} \in \mathcal{C}_j,\, b_i = \alpha} w_{j,\boldsymbol{b}} = \sum_{\boldsymbol{k} \in \mathcal{T}_j} \sum_{\boldsymbol{b} \in \mathcal{C}_j,\, \boldsymbol{\kappa}_j(\boldsymbol{b}) = \boldsymbol{k},\, b_i = \alpha} w_{j,\boldsymbol{b}} = \sum_{\boldsymbol{k} \in \mathcal{T}_j} z_{i,j,\boldsymbol{k}}^{(\alpha)} \,,$$

and thus constraint (7) is satisfied.
Next, for every $j \in \mathcal{J}$, we have by (4)

$$1 = \sum_{\boldsymbol{b} \in \mathcal{C}_j} w_{j,\boldsymbol{b}} = \sum_{\boldsymbol{k} \in \mathcal{T}_j} \sum_{\boldsymbol{b} \in \mathcal{C}_j, \boldsymbol{\kappa}_j(\boldsymbol{b}) = \boldsymbol{k}} w_{j,\boldsymbol{b}} = \sum_{\boldsymbol{k} \in \mathcal{T}_j} \sigma_{j,\boldsymbol{k}} \,,$$

and thus constraint (8) is satisfied.
Finally, for every $j \in \mathcal{J},\ \boldsymbol{k} \in \mathcal{T}_j,\ \alpha \in \Re^-$,

$$\begin{aligned} &\sum_{i \in \mathcal{I}_j,\, \beta \in \Re^-,\, \beta\mathcal{H}_{j,i} = \alpha} z_{i,j,\boldsymbol{k}}^{(\beta)} \\ &= \sum_{i \in \mathcal{I}_j,\, \beta \in \Re^-,\, \beta\mathcal{H}_{j,i} = \alpha} \ \sum_{\boldsymbol{b} \in \mathcal{C}_j,\, \boldsymbol{\kappa}_j(\boldsymbol{b}) = \boldsymbol{k},\, b_i = \beta} w_{j,\boldsymbol{b}} \\ &= \sum_{\boldsymbol{b} \in \mathcal{C}_j,\, \boldsymbol{\kappa}_j(\boldsymbol{b}) = \boldsymbol{k}} \ \sum_{i \in \mathcal{I}_j,\, b_i\mathcal{H}_{j,i} = \alpha} w_{j,\boldsymbol{b}} \\ &= \sum_{\boldsymbol{b} \in \mathcal{C}_j,\, \boldsymbol{\kappa}_j(\boldsymbol{b}) = \boldsymbol{k}} k_\alpha \cdot w_{j,\boldsymbol{b}} = k_\alpha \cdot \sigma_{j,\boldsymbol{k}} \,. \end{aligned}$$

Thus, constraint (9) is also satisfied. This completes the proof of the first part of the theorem.

2) Now assume $(\boldsymbol{f}, \boldsymbol{\sigma}, \boldsymbol{z})$ is a vertex of the polytope $\mathcal{U}$, and so all variables are rational, as are the variables $\boldsymbol{\tau}$. Next, fix some $j \in \mathcal{J}, \boldsymbol{k} \in \mathcal{T}_j$, and consider the sets

$$\mathcal{X}_0^{(\alpha)} = \left\{ \frac{\tau_{i,j,\boldsymbol{k}}^{(\alpha)}}{\sigma_{j,\boldsymbol{k}}} \,:\, i \in \mathcal{I}_j \right\} .$$

for $\alpha \in \Re^-$. By constraint (17), for each $\alpha \in \Re^-$, all the values in the set $\mathcal{X}_0^{(\alpha)}$ are rational numbers between 0 and 1. Let μ be the lowest common denominator of all the numbers in all the sets $\mathcal{X}_0^{(\alpha)}$, $\alpha \in \Re^-$. Let

$$\mathcal{X}^{(\alpha)} = \left\{ \mu \cdot \frac{\tau_{i,j,\boldsymbol{k}}^{(\alpha)}}{\sigma_{j,\boldsymbol{k}}} \,:\, i \in \mathcal{I}_j \right\} ,$$

for each $\alpha \in \Re^-$. The sets $\mathcal{X}^{(\alpha)}$ consist of integers between 0 and μ. By constraint (16), we must have that for every $\alpha \in \Re^-$, the sum of the elements in $\mathcal{X}^{(\alpha)}$ is equal to $k_\alpha \mu$. By constraint (17), we have

$$\sum_{\alpha \in \Re^-} \mu \cdot \frac{\tau_{i,j,\boldsymbol{k}}^{(\alpha)}}{\sigma_{j,\boldsymbol{k}}} \le \mu$$

for all $i \in \mathcal{I}_j$.
We now apply the result of Proposition 3.1 with $\Gamma = \mathcal{I}_j$, $M = \mu$ and with the sets $\mathcal{X}^{(\alpha)}$ defined as above (here

$N = d_j$). Set the variables $\{w_{\boldsymbol{a}} \,:\, \boldsymbol{a} \in \mathcal{C}_\Gamma^{(\boldsymbol{k})}\}$ according to Proposition 3.1.

Next, for $\boldsymbol{k} \in \mathcal{T}_j$, we show how to define the variables $\{w'_{\boldsymbol{b}} \,:\, \boldsymbol{b} \in \mathcal{C}_j,\ \boldsymbol{\kappa}_j(\boldsymbol{b}) = \boldsymbol{k}\}$. Initially, we set $w'_{\boldsymbol{b}} = 0$ for all $\boldsymbol{b} \in \mathcal{C}_j,\ \boldsymbol{\kappa}_j(\boldsymbol{b}) = \boldsymbol{k}$. Observe that the values $\mu \cdot z_{i,j,\boldsymbol{k}}^{(\beta)}/\sigma_{j,\boldsymbol{k}}$ are non-negative integers for every $i \in \mathcal{I},\ j \in \mathcal{J},\ \boldsymbol{k} \in \mathcal{T}_j,\ \beta \in \mathfrak{R}^-$.

For every $\boldsymbol{a} \in \mathcal{C}_\Gamma^{(\boldsymbol{k})}$, we define $w_{\boldsymbol{a}}$ words $\boldsymbol{b}^{(1)}, \boldsymbol{b}^{(1)}, \cdots, \boldsymbol{b}^{(w_{\boldsymbol{a}})} \in \mathcal{C}_j$. Assume some ordering on the elements $\beta \in \mathfrak{R}^-$ satisfying $\beta \mathcal{H}_{j,i} = a_i$, namely $\beta_1, \beta_2, \cdots, \beta_{\ell_0}$ for some positive integer ℓ_0. For $i \in \mathcal{I}_j$, $\boldsymbol{b}_i^{(\ell)}$ ($\ell = 1, 2, \cdots, w_{\boldsymbol{a}}$) is defined as follows: $\boldsymbol{b}_i^{(\ell)}$ is equal to β_1 for the first $\mu \cdot z_{i,j,\boldsymbol{k}}^{(\beta_1)}/\sigma_{j,\boldsymbol{k}}$ words $\boldsymbol{b}^{(1)}, \boldsymbol{b}^{(2)}, \cdots, \boldsymbol{b}^{(w_{\boldsymbol{a}})}$; $\boldsymbol{b}_i^{(\ell)}$ is equal to β_2 for the next $\mu \cdot z_{i,j,\boldsymbol{k}}^{(\beta_2)}/\sigma_{j,\boldsymbol{k}}$ words, and so on. For every $\boldsymbol{b} \in \mathcal{C}_j$ we define

$$w'_{\boldsymbol{b}} = \left| \left\{ i \in \{1, 2, \cdots, w_{\boldsymbol{a}}\} \,:\, \boldsymbol{b}^{(i)} = \boldsymbol{b} \right\} \right| .$$

Finally, for every $\boldsymbol{b} \in \mathcal{C}_j, \boldsymbol{\kappa}_j(\boldsymbol{b}) = \boldsymbol{k}$, we define

$$w_{j,\boldsymbol{b}} = \frac{\sigma_{j,\boldsymbol{k}}}{\mu} \cdot w'_{\boldsymbol{b}} .$$

Using Proposition 3.1,

$$\sum_{\boldsymbol{a} \in \mathcal{C}_\Gamma^{(\boldsymbol{k})},\ a_i = \alpha} w_{\boldsymbol{a}} = \mu \cdot \frac{\tau_{i,j,\boldsymbol{k}}^{(\alpha)}}{\sigma_{j,\boldsymbol{k}}} = \sum_{\beta \,:\, \beta \mathcal{H}_{j,i} = \alpha} \mu \cdot \frac{z_{i,j,\boldsymbol{k}}^{(\beta)}}{\sigma_{j,\boldsymbol{k}}} ,$$

and so all $\boldsymbol{b}^{(1)}, \boldsymbol{b}^{(2)}, \cdots, \boldsymbol{b}^{(w_{\boldsymbol{a}})}$ (for all $\boldsymbol{a} \in \mathcal{C}_\Gamma^{(\boldsymbol{k})}$) are well-defined. It is also straightforward to see that $\boldsymbol{b}^{(\ell)} \in \mathcal{C}_j$ for $\ell = 1, 2, \cdots, w_{\boldsymbol{a}}$. Next, we check that the newly-defined $w_{j,\boldsymbol{b}}$ satisfy (3)-(5) for every $j \in \mathcal{J},\ \boldsymbol{b} \in \mathcal{C}_j$.

It is easy to see that $w_{j,\boldsymbol{b}} \ge 0$; therefore (3) holds. By Proposition 3.1 we obtain

$$\sigma_{j,\boldsymbol{k}} = \sum_{\boldsymbol{b} \in \mathcal{C}_j,\ \boldsymbol{\kappa}_j(\boldsymbol{b}) = \boldsymbol{k}} w_{j,\boldsymbol{b}} ,$$

for all $j \in \mathcal{J}, \boldsymbol{k} \in \mathcal{T}_j$, and

$$\tau_{i,j,\boldsymbol{k}}^{(\alpha)} = \sum_{\boldsymbol{b} \in \mathcal{C}_j,\ \boldsymbol{\kappa}_j(\boldsymbol{b}) = \boldsymbol{k},\ b_i \mathcal{H}_{j,i} = \alpha} w_{j,\boldsymbol{b}} ,$$

for all $j \in \mathcal{J},\ i \in \mathcal{I}_j,\ \boldsymbol{k} \in \mathcal{T}_j,\ \alpha \in \mathfrak{R}^-$. Let $\beta \mathcal{H}_{j,i} = \alpha$. By the definition of $w_{j,\boldsymbol{b}}$ it follows that

$$\begin{aligned} &\sum_{\boldsymbol{b} \in \mathcal{C}_j,\ \boldsymbol{\kappa}(\boldsymbol{b}) = \boldsymbol{k},\ b_i = \beta} w_{j,\boldsymbol{b}} \\ &= \frac{z_{i,j,\boldsymbol{k}}^{(\beta)}}{\tau_{i,j,\boldsymbol{k}}^{(\alpha)}} \cdot \sum_{\boldsymbol{b} \in \mathcal{C}_j,\ \boldsymbol{\kappa}(\boldsymbol{b}) = \boldsymbol{k},\ b_i \mathcal{H}_{j,i} = \alpha} w_{j,\boldsymbol{b}} \;=\; z_{i,j,\boldsymbol{k}}^{(\beta)} , \end{aligned}$$

where the first equality is due to the definition of the words $\boldsymbol{b}^{(\ell)}$, $\ell = 1, 2, \cdots, w_{\boldsymbol{a}}$.

By constraint (8) we have, for all $j \in \mathcal{J}$,

$$\begin{aligned} 1 &= \sum_{\boldsymbol{k} \in \mathcal{T}_j} \sigma_{j,\boldsymbol{k}} \\ &= \sum_{\boldsymbol{k} \in \mathcal{T}_j} \sum_{\boldsymbol{b} \in \mathcal{C}_j,\ \boldsymbol{\kappa}_j(\boldsymbol{b}) = \boldsymbol{k}} w_{j,\boldsymbol{b}} \;=\; \sum_{\boldsymbol{b} \in \mathcal{C}_j} w_{j,\boldsymbol{b}} , \end{aligned}$$

thus satisfying (4).

Finally, by constraint (7) we obtain, for all $j \in \mathcal{J}, i \in \mathcal{I}_j, \beta \in \mathfrak{R}^-$,

$$\begin{aligned} f_i^{(\beta)} &= \sum_{\boldsymbol{k} \in \mathcal{T}_j} z_{i,j,\boldsymbol{k}}^{(\beta)} \\ &= \sum_{\boldsymbol{k} \in \mathcal{T}_j} \sum_{\boldsymbol{b} \in \mathcal{C}_j,\ \boldsymbol{\kappa}_j(\boldsymbol{b}) = \boldsymbol{k},\ b_i = \beta} w_{j,\boldsymbol{b}} \;=\; \sum_{\boldsymbol{b} \in \mathcal{C}_j,\ b_i = \beta} w_{j,\boldsymbol{b}} , \end{aligned}$$

thus satisfying (5).

Sketch of the Proof of Proposition 3.1

In this proof, we use a network flow approach (see [6] for background material).

The proof will be by induction on M. We set $w_{\boldsymbol{a}} = 0$ for all $\boldsymbol{a} \in \mathcal{C}_\Gamma^{(\boldsymbol{k})}$. We show that there exists a vector $\boldsymbol{a} = (a_i)_{i \in \Gamma} \in \mathcal{C}_\Gamma^{(\boldsymbol{k})}$ such that

(i) For every $i \in \Gamma$ and $\alpha \in \mathfrak{R}^-$,

$$a_i = \alpha \quad \Longrightarrow \quad x_i^{(\alpha)} > 0 .$$

(ii) If for some $i \in \Gamma$, $\sum_{\alpha \in \mathfrak{R}^-} x_i^{(\alpha)} = M$, then $a_i = \alpha$ for some $\alpha \in \mathfrak{R}^-$.

Then, we 'update' the values of $x_i^{(\alpha)}$'s and M as follows. For every $i \in \Gamma$ and $\alpha \in \mathfrak{R}^-$ with $a_i = \alpha$ we set $x_i^{(\alpha)} \leftarrow x_i^{(\alpha)} - 1$. In addition, we set $M \leftarrow M - 1$. We also set $w_{\boldsymbol{a}} \leftarrow w_{\boldsymbol{a}} + 1$.

It is easy to see that the 'updated' values of $x_i^{(\alpha)}$'s and M satisfy

$$\sum_{i \in \Gamma} x_i^{(\alpha)} = k_\alpha M$$

for all $\alpha \in \mathfrak{R}^-$, and $\sum_{\alpha \in \mathfrak{R}^-} x_i^{(\alpha)} \le M$ for all $i \in \Gamma$. Therefore, the inductive step can be applied with respect to these new values. The induction ends when the value of M is equal to zero.

It is straightforward to see that when the induction terminates, (20) and (21) hold with respect to the original values of the $x_i^{(\alpha)}$ and M.

Existence of $\boldsymbol{a}$ that satisfies (i): We construct a flow network $\mathsf{G} = (\mathsf{V}, \mathsf{E})$ as follows: $\mathsf{V} = \{s, t\} \cup \mathsf{U}_1 \cup \mathsf{U}_2$, where $\mathsf{U}_1 = \mathfrak{R}^-$ and $\mathsf{U}_2 = \Gamma$. Also set

$$\mathsf{E} = \{(s, \alpha)\}_{\alpha \in \mathfrak{R}^-} \ \cup\ \{(i, t)\}_{i \in \Gamma} \ \cup\ \{(\alpha, i)\}_{x_i^{(\alpha)} > 0} .$$

We define an integral capacity function $\mathsf{c} : \mathsf{E} \longrightarrow \mathbb{N} \cup \{+\infty\}$ as follows:

$$\mathsf{c}(e) = \begin{cases} k_\alpha & \text{if } e = (s, \alpha),\ \alpha \in \mathfrak{R}^- \\ 1 & \text{if } e = (i, t),\ i \in \Gamma \\ +\infty & \text{if } e = (\alpha, i),\ \alpha \in \mathfrak{R}^-,\ i \in \Gamma \end{cases} . \tag{22}$$

Next, apply the Ford-Fulkerson algorithm on the network $(\mathsf{G}(\mathsf{E}, \mathsf{V}), \mathsf{c})$ to produce a maximal flow $\mathsf{f}_{\max}$. Since all the values of $\mathsf{c}(e)$ are integral for all $e \in \mathsf{E}$, so the values of $\mathsf{f}_{\max}(e)$ must all be integral for every $e \in \mathsf{E}$ (see [6]).

It can be shown that the minimum cut in this graph has capacity $\mathsf{c}_{\min} = \sum_{\alpha \in \mathfrak{R}^-} k_\alpha$.

The flow $\mathsf{f}_{\max}$ in G has a value of $\sum_{\alpha \in \mathfrak{R}^-} k_\alpha$. Observe that $\mathsf{f}_{\max}((\alpha, i)) \in \{0,1\}$ for all $\alpha \in \mathfrak{R}^-$ and $i \in \Gamma$. Then, for all $i \in \Gamma$, we define

$$a_i = \begin{cases} \alpha & \text{if } \mathsf{f}_{\max}((\alpha, i)) = 1 \text{ for some } \alpha \in \mathsf{U}_1 \\ 0 & \text{otherwise} \end{cases} .$$

For this selection of $\boldsymbol{a} = (a_1, a_2, \cdots, a_N)$, we have $\boldsymbol{a} \in \mathcal{C}_\Gamma^{(\boldsymbol{k})}$ and $a_i = \alpha$ only if $x_i^{(\alpha)} > 0$.

Existence of $\boldsymbol{a}$ that satisfies (i) and (ii) simultaneously: We start with the following definition.

Definition 3.1: The vertex $i \in \mathsf{U}_2$ is called a *critical* vertex, if $\sum_{\alpha \in \mathfrak{R}^-} x_i^{(\alpha)} = M$.

In order to have (19) satisfied after the next inductive step, we have to decrease the value of $\sum_{\alpha \in \mathfrak{R}^-} x_i^{(\alpha)}$ by (exactly) 1 for every critical vertex. This is equivalent to having $\mathsf{f}_{\max}((i,t)) = 1$.

We aim to show that there exists a flow f^* of the same value, which has $\mathsf{f}^*((i,t)) = 1$ for every critical vertex i. Suppose that there is no such flow. Then, consider the maximum flow f', which has $\mathsf{f}'((i,t)) = 1$ for the *maximal possible number* of the critical vertices $i \in \mathsf{U}_2$. We assume that there is a critical vertex $i_0 \in \mathsf{U}_2$, which has $\mathsf{f}'((i_0,t)) = 0$. It is possible to show that the flow f' can be modified towards the flow f'' of the same value, such that for f'' the number of critical vertices $i \in \mathsf{U}_2$ having $\mathsf{f}''((i,t)) = 1$ is strictly larger than for f'.

It follows that there exists an integral flow f^* in $(\mathsf{G}(\mathsf{V},\mathsf{E}),\mathsf{c})$ of value $\sum_{\alpha \in \mathfrak{R}^-} k_\alpha$, such that for every critical vertex $i \in \mathsf{U}_2$, $\mathsf{f}^*((i,t)) = 1$. We define

$$a_i = \begin{cases} \alpha & \text{if } \mathsf{f}^*((\alpha, i)) = 1 \text{ for some } \alpha \in \mathsf{U}_1 \\ 0 & \text{otherwise} \end{cases} .$$

and $\boldsymbol{a} = (a_i)_{i \in \Gamma}$. For this selection of $\boldsymbol{a}$, we have $\boldsymbol{a} \in \mathcal{C}_\Gamma^{(\boldsymbol{k})}$ and the properties (i) and (ii) are satisfied. □

IV. Cascaded Polytope Representation

In this section we show that the "cascaded polytope" representation described in [4] and [5] can be extended to non-binary codes in a straightforward manner. Below, we elaborate on the details.

For $j \in \mathcal{J}$, consider the j-th row $\mathcal{H}_j$ of the parity-check matrix $\mathcal{H}$ over $\mathfrak{R}$, and recall that

$$\mathcal{C}_j = \left\{ (b_i)_{i \in \mathcal{I}_j} \; : \; \sum_{i \in \mathcal{I}_j} b_i \cdot \mathcal{H}_{j,i} = 0 \right\} .$$

Assume that $\mathcal{I}_j = \{i_1, i_2, \cdots, i_{d_j}\}$ and denote $\mathcal{L}_j = \{1, 2, \cdots, d_j - 3\}$. We introduce new variables $\boldsymbol{\chi}^j = (\chi_i^j)_{i \in \mathcal{L}_j}$ and denote $\boldsymbol{\chi} = (\boldsymbol{\chi}^j)_{j \in \mathcal{J}}$.

We define a new linear code $\mathcal{C}_j^{(\chi)}$ of length $2d_j - 3$ by $(d_j - 2) \times (2d_j - 3)$ parity-check matrix associated with the following set of parity-check equations over $\mathfrak{R}$:

1) $$b_{i_1} \mathcal{H}_{j,i_1} + b_{i_2} \mathcal{H}_{j,i_2} + \chi_1^j = 0 \; . \tag{23}$$

2) For every $\ell = 1, 2, \cdots, d_j - 4$,
$$-\chi_\ell^j + b_{i_{\ell+2}} \mathcal{H}_{j,i_{\ell+2}} + \chi_{\ell+1}^j = 0 \; . \tag{24}$$

3) $$-\chi_{d_j-3}^j + b_{i_{d_j-1}} \mathcal{H}_{j,i_{d_j-1}} + b_{i_{d_j}} \mathcal{H}_{j,i_{d_j}} = 0 \; . \tag{25}$$

We also define a linear code $\mathcal{C}^{(\chi)}$ of length $n + \sum_{j \in \mathcal{J}} (d_j - 3)$ defined by $(\sum_{j \in \mathcal{J}} (d_j - 2)) \times (n + \sum_{j \in \mathcal{J}} (d_j - 3))$ parity-check matrix $\mathcal{F}$ associated with all the sets of parity-check equations (23)-(25) (for all $j \in \mathcal{J}$).

Theorem 4.1: The vector $(b_i)_{i \in \mathcal{I}_j} \in \mathfrak{R}^{d_j}$ is a codeword of $\mathcal{C}_j$ if and only if there exists some vector $\boldsymbol{\chi}^j \in \mathfrak{R}^{d_j - 3}$ such that $((b_i)_{i \in \mathcal{I}_j} \mid \boldsymbol{\chi}^j) \in \mathcal{C}_j^{(\chi)}$.

We denote by $\mathcal{S}$ the polytope corresponding to the LP relaxation problem (3)-(5) for the code $\mathcal{C}^{(\chi)}$ with the parity-check matrix $\mathcal{F}$. Let $(\boldsymbol{b}, \boldsymbol{\chi})$ be a word in $\mathcal{C}^{(\chi)}$, where $\boldsymbol{b} \in \mathcal{C}$. It is natural to represent points in $\mathcal{S}$ as $((\boldsymbol{f}, \boldsymbol{h}), \boldsymbol{z})$, where $\boldsymbol{f} = (f_i^{(\alpha)})_{i \in \mathcal{I}, \alpha \in \mathfrak{R}^-}$ and $\boldsymbol{h} = (h_{j,i}^{(\alpha)})_{j \in \mathcal{J}, i \in \mathcal{L}_j, \alpha \in \mathfrak{R}^-}$ are vectors of indicators corresponding to the entries b_i ($i \in \mathcal{I}$) in $\boldsymbol{b}$ and χ_i^j ($j \in \mathcal{J}$, $i \in \mathcal{L}_j$) in $\boldsymbol{\chi}$, respectively.

Theorem 4.2: The set $\bar{\mathcal{S}} = \{ \boldsymbol{f} : \exists \, \boldsymbol{h}, \boldsymbol{z} \text{ s.t. } ((\boldsymbol{f}, \boldsymbol{h}), \boldsymbol{z}) \in \mathcal{S} \}$ is equal to the set $\bar{\mathcal{Q}} = \{ \boldsymbol{f} : \exists \, \boldsymbol{w} \text{ s.t. } (\boldsymbol{f}, \boldsymbol{w}) \in \mathcal{Q} \}$, and therefore, optimizing the linear cost function (2) over $\mathcal{S}$ is equivalent to optimizing it over $\mathcal{Q}$.

It follows from Theorem 4.2 that the polytope $\mathcal{S}$ equivalently describes the code $\mathcal{C}$. This description has at most $n + m \cdot (d-3)$ variables and $m \cdot (d-2)$ parity-check equations. However, the number of variables participating in every parity-check equation is at most 3. Therefore, the total number of variables and of equations in the respective LP problem will be bounded from above by

$$(n + m(d-3))(q-1) + m(d-2) \cdot q^2$$

and
$$m(d-2)(q^2 + 3q - 2) \; .$$

The polytope representation in this section, when used with the LP problem in [3], leads to a polynomial-time decoder for a wide variety of classical non-binary codes. Its performance under LP decoding is yet to be studied.

Acknowledgements

The authors wish to thank O. Milenkovic for interesting discussions. This work was supported by the Claude Shannon Institute for Discrete Mathematics, Coding and Cryptography (Science Foundation Ireland Grant 06/MI/006).

References

[1] J. Feldman, *Decoding Error-Correcting Codes via Linear Programming*, Ph.D. Thesis, Massachusetts Institute of Technology, Sep. 2003.

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

[3] M.F. Flanagan, V. Skachek, E. Byrne, M. Greferath, *Linear-programming Decoding of Non-binary Linear Codes, Proc. 7th Int. ITG Confer. on Source and Channel Coding (SCC)*, Jan. 2008, Ulm, Germany. Available also at `http://arxiv.org/abs/0707.4360`.

[4] M. Chertkov, M. Stepanov, *Pseudo-codeword Landscape, Proc. IEEE Int. Symp. on Inform. Theory (ISIT), June 2007, p.1546-1550,* Nice, France.

[5] K. Yang, X. Wang, J. Feldman, *Cascaded Formulation of the Fundamental Polytope of General Linear Block Codes, Proc. IEEE Int. Symp. on Inform. Theory (ISIT), June 2007, p.1361-1365,* Nice, France.

[6] T.H. Cormen, C.E. Leiserson, R.L. Rivest, C. Stein, *Introduction to Algorithms*, second edition, MIT Press and McGraw-Hill, 2001.