

Codeword-Independent Performance of Nonbinary Linear Codes Under Linear-Programming and Sum-Product Decoding

Mark F. Flanagan

DEIS/CNIT

University of Bologna

via Venezia 52, 47023 Cesena (FC), Italy

Email: mark.flanagan@ieee.org

Abstract—A coded modulation system is considered in which nonbinary coded symbols are mapped directly to nonbinary modulation signals. It is proved that if the modulator-channel combination satisfies a particular symmetry condition, the codeword error rate performance is independent of the transmitted codeword. It is shown that this result holds for both linear-programming decoders and sum-product decoders. In particular, this provides a natural modulation mapping for nonbinary codes mapped to PSK constellations for transmission over memoryless channels such as AWGN channels or flat fading channels with AWGN.

I. INTRODUCTION

Low-density parity check (LDPC) codes [1], as well as their nonbinary counterparts [2] have been shown to exhibit excellent error-correcting performance when decoded by the traditional *sum-product* (SP) decoding algorithm. In [3], Feldman *et al.* introduced the idea of *linear-programming* (LP) decoding of LDPC codes. This was later generalized to nonbinary codes in [4].

For classical coded modulation systems, *geometric uniformity* [5] was identified as a symmetry condition which, if satisfied, guarantees codeword error rate performance independent of the transmitted codeword, where maximum-likelihood (ML) decoding is assumed. Some recent coded modulation schemes with SP decoding used this symmetry condition for design [6]. An analogous symmetry condition was defined in [7] for binary codes over $GF(2)$ with SP decoding; this was extended to nonbinary codes over $GF(q)$ by invoking the concept of *coset* LDPC codes [2].

In this work it is shown that for the cases of LP and SP decoding of linear codes over rings, there exists a symmetry condition under which the codeword error rate performance is independent of the transmitted codeword (for the case of LP decoding this theorem generalizes [3, Theorem 6], and is stated in [4]). This provides a condition somewhat akin to geometric uniformity for state-of-the-art nonbinary coded modulation systems.

II. GENERAL FRAMEWORK

We consider codes over finite rings (this includes codes over finite fields, but may be more general). Denote by \mathfrak{R}

a ring with q elements, by 0 its additive identity, and let $\mathfrak{R}^- = \mathfrak{R} \setminus \{0\}$. Let $\mathcal{C} = \{c \in \mathfrak{R}^n : c\mathcal{H}^T = \mathbf{0}\}$ be a linear code defined with respect to the $m \times n$ parity-check matrix \mathcal{H} over \mathfrak{R} . Denote the set of column indices and the set of row indices of \mathcal{H} by $\mathcal{I} = \{1, 2, \dots, n\}$ and $\mathcal{J} = \{1, 2, \dots, m\}$, respectively. For $j \in \mathcal{J}$, let $\mathcal{H}_j^{(r)}$ denote the j -th row of \mathcal{H} , and for $i \in \mathcal{I}$, let $\mathcal{H}_i^{(c)}$ denote the i -th column. Denote by $\text{supp}(c)$ the support of a vector c . For each $i \in \mathcal{I}$, let $\mathcal{J}_i = \text{supp}(\mathcal{H}_i^{(c)})$ and for each $j \in \mathcal{J}$, let $\mathcal{I}_j = \text{supp}(\mathcal{H}_j^{(r)})$. Also let $\mathcal{A}_{j,i} = \mathcal{I}_j \setminus \{i\}$ and $\mathcal{D}_{j,i} = \mathcal{J}_i \setminus \{j\}$.

Given any $c \in \mathfrak{R}^n$, we say that parity check $j \in \mathcal{J}$ is *satisfied* by c if and only if

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

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 . We define the projection mapping for parity check $j \in \mathcal{J}$ by

$$\mathbf{x}_j(c) = (c_i)_{i \in \mathcal{I}_j}$$

Then, given any $c \in \mathfrak{R}^n$, we may say that parity check $j \in \mathcal{J}$ is satisfied by c if and only if

$$\mathbf{x}_j(c) \in \mathcal{C}_j \quad (2)$$

since (1) and (2) are equivalent. Also, we say that the vector c is a codeword of \mathcal{C} , writing $c \in \mathcal{C}$, if and only if all parity checks $j \in \mathcal{J}$ are satisfied by c .

Assume that the codeword $\bar{c} = (\bar{c}_1, \bar{c}_2, \dots, \bar{c}_n) \in \mathcal{C}$ has been transmitted over a q -ary input memoryless channel, and a corrupted word $\mathbf{y} = (y_1, y_2, \dots, y_n) \in \Sigma^n$ has been received. Here Σ denotes the set of channel output symbols; we assume that this set either has finite cardinality, or is equal to \mathbb{R}^l or \mathbb{C}^l for some integer $l \geq 1$. In practice, this channel may represent the combination of modulator and physical channel. It is assumed hereafter that all information words are equally

probable, and so all codewords are transmitted with equal probability.

Next we set up some definitions and notation. We define the mapping

$$\xi : \mathfrak{R} \mapsto \{0, 1\}^{q-1} \subset \mathbb{R}^{q-1}$$

by

$$\xi(\alpha) = \mathbf{x} = (x^{(\gamma)})_{\gamma \in \mathfrak{R}^-}$$

such that, for each $\gamma \in \mathfrak{R}^-$,

$$x^{(\gamma)} = \begin{cases} 1 & \text{if } \gamma = \alpha \\ 0 & \text{otherwise.} \end{cases}$$

We note that the mapping ξ is one-to-one, and its image is the set of binary vectors of length $q-1$ with Hamming weight 0 or 1. Building on this, we also define

$$\Xi : \mathfrak{R}^n \mapsto \{0, 1\}^{(q-1)n} \subset \mathbb{R}^{(q-1)n}$$

according to

$$\Xi(\mathbf{c}) = (\xi(c_1) \mid \xi(c_2) \mid \cdots \mid \xi(c_n))$$

We note that Ξ is also one-to-one.

Now, for vectors $\mathbf{f} \in \mathbb{R}^{(q-1)n}$, we adopt the notation

$$\mathbf{f} = (\mathbf{f}_1 \mid \mathbf{f}_2 \mid \cdots \mid \mathbf{f}_n)$$

where

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

In particular, we define $\lambda \in \mathbb{R}^{(q-1)n}$ by setting, for each $i \in \mathcal{I}$, $\alpha \in \mathfrak{R}^-$,

$$\lambda_i^{(\alpha)} = \log \left(\frac{p(y_i|0)}{p(y_i|\alpha)} \right)$$

and $p(y_i|c_i)$ denotes the channel output probability (density) conditioned on the channel input.

Also, we may use this notation to write the inverse of Ξ as

$$\Xi^{-1}(\mathbf{f}) = (\xi^{-1}(\mathbf{f}_1), \xi^{-1}(\mathbf{f}_2), \cdots, \xi^{-1}(\mathbf{f}_n))$$

III. DECODING ALGORITHMS

A. Linear-Programming Decoder

The linear-programming (LP) decoder of [4] operates as follows. The linear program described here is equivalent to that given in [4]; however, some changes of notation have been made in order to facilitate the proof to come in section IV. The variables of the LP are

$$f_i^{(\alpha)} \text{ for each } i \in \mathcal{I}, \alpha \in \mathfrak{R}^-$$

and

$$w_{j,\mathbf{b}} \text{ for each } j \in \mathcal{J}, \mathbf{b} \in C_j$$

and the constraints are

$$\forall j \in \mathcal{J}, \forall \mathbf{b} \in C_j, w_{j,\mathbf{b}} \geq 0 \quad (3)$$

and

$$\forall j \in \mathcal{J}, \sum_{\mathbf{b} \in C_j} w_{j,\mathbf{b}} = 1 \quad (4)$$

and

$$\begin{aligned} \forall j \in \mathcal{J}, \forall i \in \mathcal{I}_j, \forall \alpha \in \mathfrak{R}^-, \\ f_i^{(\alpha)} = \sum_{\mathbf{b} \in C_j, b_i = \alpha} w_{j,\mathbf{b}} \end{aligned} \quad (5)$$

The set of points (\mathbf{f}, \mathbf{w}) which satisfy (3)-(5) form a polytope denoted by \mathcal{Q} . The cost function to be minimized over this polytope is $F(\mathbf{f}) = \lambda \mathbf{f}^T$, and the minimizer is denoted by $\hat{\mathbf{f}}$. If $\hat{\mathbf{f}} \in \{0, 1\}^{(q-1)n}$, the output is the codeword $\Xi^{-1}(\hat{\mathbf{f}})$ (it is proved in [4] that this must be the maximum-likelihood codeword). Otherwise, the decoder outputs a ‘decoding failure’.

B. Sum-Product Decoder

The sum-product (SP) decoder operates as follows. Note that in practice, computations are usually carried out in the log-domain, but this does not affect our analysis.

Initializing

$$m_i(\alpha) = p(y_i|\alpha) \quad \forall i \in \mathcal{I}, \forall \alpha \in \mathfrak{R} \quad (6)$$

and

$$m_{j,i}^{D,0}(\alpha) = 1 \quad \forall j \in \mathcal{J}, \forall i \in \mathcal{I}_j, \forall \alpha \in \mathfrak{R} \quad (7)$$

N iterations of fully parallel SP decoding may be represented by the following recursive formulas. For each $k = 1, 2, \dots, N$,

$$m_{j,i}^{U,k}(\alpha) = m_i(\alpha) \cdot \prod_{l \in \mathcal{D}_{j,i}} m_{l,i}^{D,k-1}(\alpha) \quad (8)$$

for each $j \in \mathcal{J}, i \in \mathcal{I}_j, \alpha \in \mathfrak{R}$, and

$$m_{j,i}^{D,k}(\alpha) = \sum_{\substack{l \in \mathcal{A}_{j,i} \\ d_l \mathcal{H}_{j,i} = -\alpha \mathcal{H}_{j,i}}} \left\{ \prod_{l \in \mathcal{A}_{j,i}} m_{j,l}^{U,k}(d_l) \right\} \quad (9)$$

for each $j \in \mathcal{J}, i \in \mathcal{I}_j, \alpha \in \mathfrak{R}$. Finally, decisions are made via

$$g_i(\alpha) = m_i(\alpha) \cdot \prod_{j \in \mathcal{J}_i} m_{j,i}^{D,N}(\alpha) \quad \forall i \in \mathcal{I}, \forall \alpha \in \mathfrak{R} \quad (10)$$

and

$$h_i = \arg \max_{\alpha \in \mathfrak{R}} \{g_i(\alpha)\} \quad \forall i \in \mathcal{I} \quad (11)$$

The output of the decoder is then $\mathbf{h} = (h_1, h_2, \dots, h_n)$.

IV. MAIN RESULT

Symmetry Condition.

For each $\beta \in \mathfrak{R}$, there exists a bijection

$$\tau_\beta : \Sigma \longrightarrow \Sigma$$

such that the channel output probability (density) conditioned on the channel input satisfies

$$p(y|\alpha) = p(\tau_\beta(y)|\alpha - \beta) \quad (12)$$

for all $y \in \Sigma, \alpha \in \mathfrak{R}$. When Σ is equal to \mathbb{R}^l or \mathbb{C}^l for $l \geq 1$, the mapping τ_β is assumed to be isometric with respect to Euclidean distance in Σ , for every $\beta \in \mathfrak{R}$.

In the following, *codeword error* is defined as the event where the decoder output is not equal to the transmitted codeword.

Theorem 4.1: Under the stated symmetry condition, the probability of codeword error is independent of the transmitted codeword

- (a) under linear-programming decoding
- (b) under sum-product decoding.

Proof: We shall prove the theorem for the case where Σ has infinite cardinality; the case of discrete Σ may be handled similarly. Fix some codeword $\mathbf{c} \in \mathcal{C}$, $\mathbf{c} \neq \mathbf{0}$. We wish to prove that

$$\Pr(\text{Err} | \mathbf{c}) = \Pr(\text{Err} | \mathbf{0})$$

where $\Pr(\text{Err} | \mathbf{c})$ denotes the probability of codeword error given that the codeword \mathbf{c} was transmitted.

Now

$$\Pr(\text{Err} | \mathbf{c}) = \Pr(\mathbf{y} \in B(\mathbf{c}) | \mathbf{c})$$

where $B(\mathbf{c})$ is the set of all receive words which may cause codeword error, given that \mathbf{c} was transmitted. Also

$$\Pr(\text{Err} | \mathbf{0}) = \Pr(\mathbf{y} \in B(\mathbf{0}) | \mathbf{0})$$

So we write

$$\Pr(\text{Err} | \mathbf{c}) = \int_{\mathbf{y} \in B(\mathbf{c})} p(\mathbf{y} | \mathbf{c}) d\mathbf{y} \quad (13)$$

and

$$\Pr(\text{Err} | \mathbf{0}) = \int_{\tilde{\mathbf{y}} \in B(\mathbf{0})} p(\tilde{\mathbf{y}} | \mathbf{0}) d\tilde{\mathbf{y}} \quad (14)$$

Now, setting $\alpha = \beta$ in the symmetry condition (12) yields

$$p(y|\beta) = p(\tau_\beta(y)|0) \quad (15)$$

for any $y \in \Sigma$, $\beta \in \mathfrak{R}$.

We now define $\tilde{\mathbf{y}} = \mathbf{G}(\mathbf{y})$ as follows. For every $i \in \mathcal{I}$, if $c_i = \beta \in \mathfrak{R}$ then

$$\tilde{y}_i = \tau_\beta(y_i)$$

We note that \mathbf{G} is a bijection from the set Σ^n to itself, and that if $\mathbf{y}, \mathbf{z} \in \Sigma^n$ and $c_i = \beta \in \mathfrak{R}$ then

$$\|y_i - z_i\|^2 = \|\tau_\beta(y_i) - \tau_\beta(z_i)\|^2$$

and so

$$\|\mathbf{G}(\mathbf{y}) - \mathbf{G}(\mathbf{z})\|^2 = \|\mathbf{y} - \mathbf{z}\|^2$$

i.e. \mathbf{G} is isometric with respect to Euclidean distance in Σ^n .

We prove that the integral (13) may be transformed to (14) via the substitution $\tilde{\mathbf{y}} = \mathbf{G}(\mathbf{y})$. First, we have

$$\begin{aligned} p(\mathbf{y} | \mathbf{c}) &= \prod_{i \in \mathcal{I}} p(y_i | c_i) \\ &= \prod_{\beta \in \mathfrak{R}} \prod_{i \in \mathcal{I}, c_i = \beta} p(y_i | \beta) \\ &= \prod_{\beta \in \mathfrak{R}} \prod_{i \in \mathcal{I}, c_i = \beta} p(\tau_\beta(y_i) | 0) \\ &= \prod_{\beta \in \mathfrak{R}} \prod_{i \in \mathcal{I}, c_i = \beta} p(\tilde{y}_i | 0) \\ &= \prod_{i \in \mathcal{I}} p(\tilde{y}_i | 0) \\ &= p(\tilde{\mathbf{y}} | \mathbf{0}) \end{aligned}$$

Since \mathbf{G} is isometric with respect to Euclidean distance in Σ^n , it follows that the Jacobian determinant of the transformation is equal to unity. Therefore, to complete the proof, we need only show that

$$\mathbf{y} \in B(\mathbf{c}) \text{ if and only if } \tilde{\mathbf{y}} \in B(\mathbf{0})$$

We prove this separately for the two cases of linear-programming and sum-product decoding.

(a) *Under linear-programming decoding:*

Here

$$B(\mathbf{c}) = \{\mathbf{y} \in \Sigma^n : \exists(\mathbf{f}, \mathbf{w}) \in \mathcal{Q}, \mathbf{f} \neq \Xi(\mathbf{c}) \text{ with } \lambda \mathbf{f}^T \leq \lambda \Xi(\mathbf{c})^T\}$$

Recall that here λ is a function of \mathbf{y} via

$$\lambda_i^{(\alpha)} = \log \left(\frac{p(y_i|0)}{p(y_i|\alpha)} \right) \quad (16)$$

for $i \in \mathcal{I}$, $\alpha \in \mathfrak{R}^-$. Also

$$B(\mathbf{0}) = \{\tilde{\mathbf{y}} \in \Sigma^n : \exists(\tilde{\mathbf{f}}, \tilde{\mathbf{w}}) \in \mathcal{Q}, \tilde{\mathbf{f}} \neq \Xi(\mathbf{0}) \text{ with } \tilde{\lambda} \tilde{\mathbf{f}}^T \leq \tilde{\lambda} \Xi(\mathbf{0})^T\}$$

Here $\tilde{\lambda}$ is a function of $\tilde{\mathbf{y}}$ via

$$\tilde{\lambda}_i^{(\alpha)} = \log \left(\frac{p(\tilde{y}_i|0)}{p(\tilde{y}_i|\alpha)} \right) \quad (17)$$

for $i \in \mathcal{I}$, $\alpha \in \mathfrak{R}^-$. We begin by relating the elements of λ (defined by (16)) to the elements of $\tilde{\lambda}$ (defined by (17)). Let $i \in \mathcal{I}$, $\alpha \in \mathfrak{R}^-$. Suppose $c_i = \beta \in \mathfrak{R}$. We then have

$$\begin{aligned} \lambda_i^{(\alpha)} &= \log \left(\frac{p(y_i|0)}{p(y_i|\alpha)} \right) \\ &= \log \left(\frac{p(\tau_\beta(y_i) | -\beta)}{p(\tau_\beta(y_i) | \alpha - \beta)} \right) \\ &= \log \left(\frac{p(\tilde{y}_i | -\beta)}{p(\tilde{y}_i | \alpha - \beta)} \right) \end{aligned}$$

This yields

$$\lambda_i^{(\alpha)} = \begin{cases} \tilde{\lambda}_i^{(\alpha)} & \text{if } \beta = 0 \\ -\tilde{\lambda}_i^{(-\alpha)} & \text{if } \alpha = \beta \\ \tilde{\lambda}_i^{(\alpha-\beta)} - \tilde{\lambda}_i^{(-\beta)} & \text{otherwise.} \end{cases}$$

Next, for any point $(\mathbf{f}, \mathbf{w}) \in \mathcal{Q}$ we define a new point $(\tilde{\mathbf{f}}, \tilde{\mathbf{w}})$ as follows. For all $i \in \mathcal{I}$, $\alpha \in \mathfrak{R}^-$, if $c_i = \beta \in \mathfrak{R}$ then

$$\tilde{f}_i^{(\alpha)} = \begin{cases} 1 - \sum_{\gamma \in \mathfrak{R}^-} f_i^{(\gamma)} & \text{if } \alpha = -\beta \\ f_i^{(\alpha+\beta)} & \text{otherwise.} \end{cases} \quad (18)$$

For all $j \in \mathcal{J}$, $\mathbf{r} \in \mathcal{C}_j$ we define

$$\tilde{w}_{j,r} = w_{j,b}$$

where

$$\mathbf{b} = \mathbf{r} + \mathbf{x}_j(\mathbf{c})$$

Next we prove that for every $(\mathbf{f}, \mathbf{w}) \in \mathcal{Q}$, the new point $(\tilde{\mathbf{f}}, \tilde{\mathbf{w}})$ lies in \mathcal{Q} and thus is a feasible solution for the LP. Constraints (3) and (4) obviously hold from the definition of

$\tilde{\mathbf{w}}$. To verify (5), we let $j \in \mathcal{J}$, $i \in \mathcal{I}_j$ and $\alpha \in \mathfrak{R}^-$. We also let $c_i = \beta \in \mathfrak{R}$. We now check two cases:

- If $\alpha = -\beta$,

$$\begin{aligned} \tilde{f}_i^{(\alpha)} &= 1 - \sum_{\gamma \in \mathfrak{R}^-} f_i^{(\gamma)} \\ &= \sum_{\mathbf{b} \in \mathcal{C}_j} w_{j,\mathbf{b}} - \sum_{\gamma \in \mathfrak{R}^-} \sum_{\mathbf{b} \in \mathcal{C}_j, b_i = \gamma} w_{j,\mathbf{b}} \\ &= \sum_{\mathbf{b} \in \mathcal{C}_j, b_i = 0} w_{j,\mathbf{b}} \\ &= \sum_{\mathbf{r} \in \mathcal{C}_j, r_i = \alpha} \tilde{w}_{j,\mathbf{r}} \end{aligned}$$

- If $\alpha \neq -\beta$,

$$\begin{aligned} \tilde{f}_i^{(\alpha)} = f_i^{(\alpha+\beta)} &= \sum_{\mathbf{b} \in \mathcal{C}_j, b_i = \alpha+\beta} w_{j,\mathbf{b}} \\ &= \sum_{\mathbf{r} \in \mathcal{C}_j, r_i = \alpha} \tilde{w}_{j,\mathbf{r}} \end{aligned}$$

Therefore $(\tilde{\mathbf{f}}, \tilde{\mathbf{w}}) \in \mathcal{Q}$, i.e. $(\tilde{\mathbf{f}}, \tilde{\mathbf{w}})$ is a feasible solution for the LP. We write $(\tilde{\mathbf{f}}, \tilde{\mathbf{w}}) = \mathbf{L}(\tilde{\mathbf{f}}, \tilde{\mathbf{w}})$. We also note that the mapping \mathbf{L} is a bijection from \mathcal{Q} to itself; this is easily shown by verifying the inverse

$$f_i^{(\alpha)} = \begin{cases} 1 - \sum_{\gamma \in \mathfrak{R}^-} \tilde{f}_i^{(\gamma)} & \text{if } \alpha = \beta \\ \tilde{f}_i^{(\alpha-\beta)} & \text{otherwise} \end{cases} \quad (19)$$

for all $i \in \mathcal{I}$, $\alpha \in \mathfrak{R}^-$, and

$$w_{j,\mathbf{b}} = \tilde{w}_{j,\mathbf{r}}$$

where

$$\mathbf{r} = \mathbf{b} - \mathbf{x}_j(\mathbf{c})$$

for all $j \in \mathcal{J}$, $\mathbf{b} \in \mathcal{C}_j$.

We now prove that for every $(\mathbf{f}, \mathbf{w}) \in \mathcal{Q}$, $(\tilde{\mathbf{f}}, \tilde{\mathbf{w}}) = \mathbf{L}(\mathbf{f}, \mathbf{w})$ satisfies

$$\lambda \mathbf{f}^T - \lambda \Xi(\mathbf{c})^T = \tilde{\lambda} \tilde{\mathbf{f}}^T - \tilde{\lambda} \Xi(\mathbf{0})^T \quad (20)$$

We achieve this by proving

$$\lambda_i \mathbf{f}_i^T - \lambda_i \xi(c_i)^T = \tilde{\lambda}_i \tilde{\mathbf{f}}_i^T - \tilde{\lambda}_i \xi(0)^T \quad (21)$$

for every $i \in \mathcal{I}$. We may then obtain (20) by summing (21) over $i \in \mathcal{I}$. Let $c_i = \beta \in \mathfrak{R}$. We consider two cases:

- If $\beta = 0$, (21) becomes

$$\lambda_i \mathbf{f}_i^T = \tilde{\lambda}_i \tilde{\mathbf{f}}_i^T$$

which holds since in this case $\tilde{\lambda}_i^{(\alpha)} = \lambda_i^{(\alpha)}$ and $\tilde{f}_i^{(\alpha)} = f_i^{(\alpha)}$ for all $\alpha \in \mathfrak{R}^-$.

- If $\beta \neq 0$,

$$\begin{aligned} \lambda_i \mathbf{f}_i^T - \lambda_i \xi(c_i)^T &= \sum_{\gamma \in \mathfrak{R}^-} \lambda_i^{(\gamma)} f_i^{(\gamma)} - \lambda_i^{(\beta)} \\ &= \sum_{\substack{\gamma \in \mathfrak{R}^- \\ \gamma \neq \beta}} \left(\tilde{\lambda}_i^{(\gamma-\beta)} - \tilde{\lambda}_i^{(-\beta)} \right) f_i^{(\gamma)} - \tilde{\lambda}_i^{(-\beta)} f_i^{(\beta)} + \tilde{\lambda}_i^{(-\beta)} \\ &= \sum_{\substack{\alpha \in \mathfrak{R}^- \\ \alpha \neq -\beta}} \tilde{\lambda}_i^{(\alpha)} f_i^{(\alpha+\beta)} + \tilde{\lambda}_i^{(-\beta)} \left(1 - \sum_{\gamma \in \mathfrak{R}^-} f_i^{(\gamma)} \right) \\ &= \sum_{\alpha \in \mathfrak{R}^-} \tilde{\lambda}_i^{(\alpha)} \tilde{f}_i^{(\alpha)} \\ &= \tilde{\lambda}_i \tilde{\mathbf{f}}_i^T - \tilde{\lambda}_i \xi(0)^T \end{aligned}$$

where we have made use of the substitution $\alpha = \gamma - \beta$ in the third line. Therefore (21) holds, proving (20).

Finally, we note that it is easy to show, using (18) and (19), that $\mathbf{f} = \Xi(\mathbf{c})$ if and only if $\tilde{\mathbf{f}} = \Xi(\mathbf{0})$.

Putting together these results, we may make the following statement. Suppose we are given $\mathbf{y}, \tilde{\mathbf{y}} \in \Sigma^n$ with $\tilde{\mathbf{y}} = \mathbf{G}(\mathbf{y})$. Then the point $(\mathbf{f}, \mathbf{w}) \in \mathcal{Q}$ satisfies $\mathbf{f} \neq \Xi(\mathbf{c})$ and $\lambda \mathbf{f}^T \leq \lambda \Xi(\mathbf{c})^T$ if and only if the point $(\tilde{\mathbf{f}}, \tilde{\mathbf{w}}) = \mathbf{L}(\mathbf{f}, \mathbf{w}) \in \mathcal{Q}$ satisfies $\tilde{\mathbf{f}} \neq \Xi(\mathbf{0})$ and $\tilde{\lambda} \tilde{\mathbf{f}}^T \leq \tilde{\lambda} \Xi(\mathbf{0})^T$. This statement, along with the fact that both \mathbf{G} and \mathbf{L} are bijective, proves that

$$\mathbf{y} \in B(\mathbf{c}) \text{ if and only if } \tilde{\mathbf{y}} \in B(\mathbf{0})$$

This completes the proof of the theorem for the case of LP decoding.

(b) *Under Sum-Product Decoding:*

Recall that all decoder variables appearing in equations (6)-(11) are functions of \mathbf{y} via (6). For any such variable x , let \tilde{x} denote the corresponding variable with $\tilde{\mathbf{y}}$ as input. Then we have, for all $i \in \mathcal{I}$, $\alpha \in \mathfrak{R}$, where $c_i = \beta$,

$$\begin{aligned} m_i(\alpha) &= p(y_i | \alpha) = p(\tau_\beta(y_i) | \alpha - \beta) \\ &= p(\tilde{y}_i | \alpha - c_i) = \tilde{m}_i(\alpha - c_i) \end{aligned}$$

Next we prove by induction that for all $k = 0, 1, \dots, N$,

$$m_{j,i}^{D,k}(\alpha) = \tilde{m}_{j,i}^{D,k}(\alpha - c_i) \quad (22)$$

for all $j \in \mathcal{J}$, $i \in \mathcal{I}_j$, $\alpha \in \mathfrak{R}$. This result holds for the base case $k = 0$ because from (7)

$$m_{j,i}^{D,0}(\alpha) = \tilde{m}_{j,i}^{D,0}(\alpha) = 1 \quad \forall j \in \mathcal{J}, \forall i \in \mathcal{I}_j, \forall \alpha \in \mathfrak{R}$$

Assuming that (22) holds for some $k = r - 1 \in \{0, 1, \dots, N - 1\}$ (and for all $j \in \mathcal{J}$, $i \in \mathcal{I}_j$, $\alpha \in \mathfrak{R}$), we obtain by (8)

$$\begin{aligned} m_{j,i}^{U,r}(\alpha) &= m_i(\alpha) \cdot \prod_{l \in \mathcal{D}_{j,i}} m_{l,i}^{D,r-1}(\alpha) \\ &= \tilde{m}_i(\alpha - c_i) \cdot \prod_{l \in \mathcal{D}_{j,i}} \tilde{m}_{l,i}^{D,r-1}(\alpha - c_i) \\ &= \tilde{m}_{j,i}^{U,r}(\alpha - c_i) \end{aligned}$$

for all $j \in \mathcal{J}$, $i \in \mathcal{I}_j$, $\alpha \in \mathfrak{R}$. So, by (9),

$$\begin{aligned} m_{j,i}^{D,r}(\alpha) &= \sum_{\Sigma_{l \in \mathcal{A}_{j,i}} d_l \mathcal{H}_{j,l} = -\alpha \mathcal{H}_{j,i}} \left\{ \prod_{l \in \mathcal{A}_{j,i}} m_{j,l}^{U,r}(d_l) \right\} \\ &= \sum_{\Sigma_{l \in \mathcal{A}_{j,i}} d_l \mathcal{H}_{j,l} = -\alpha \mathcal{H}_{j,i}} \left\{ \prod_{l \in \mathcal{A}_{j,i}} \tilde{m}_{j,l}^{U,r}(d_l - c_l) \right\} \\ &= \sum_{\Sigma_{l \in \mathcal{A}_{j,i}} b_l \mathcal{H}_{j,l} = -(\alpha - c_i) \mathcal{H}_{j,i}} \left\{ \prod_{l \in \mathcal{A}_{j,i}} \tilde{m}_{j,l}^{U,r}(b_l) \right\} \\ &= \tilde{m}_{j,i}^{D,r}(\alpha - c_i) \end{aligned}$$

for all $j \in \mathcal{J}$, $i \in \mathcal{I}_j$, $\alpha \in \mathfrak{R}$, where we have made the substitution $b_l = d_l - c_l$ for each $l \in \mathcal{I}_j$, and used the fact that $\sum_{l \in \mathcal{A}_{j,i}} c_l \mathcal{H}_{j,l} = -c_i \mathcal{H}_{j,i}$ since $c \in \mathcal{C}$. It follows by the principle of induction that (22) holds for every $k = 0, 1, \dots, N$, $j \in \mathcal{J}$, $i \in \mathcal{I}_j$, $\alpha \in \mathfrak{R}$. Therefore by (10)

$$\begin{aligned} g_i(\alpha) &= m_i(\alpha) \cdot \prod_{j \in \mathcal{J}_i} m_{j,i}^{D,N}(\alpha) \\ &= \tilde{m}_i(\alpha - c_i) \cdot \prod_{j \in \mathcal{J}_i} \tilde{m}_{j,i}^{D,N}(\alpha - c_i) \\ &= \tilde{g}_i(\alpha - c_i) \end{aligned}$$

for all $i \in \mathcal{I}$, $\alpha \in \mathfrak{R}$, and so by (11), $\tilde{h}_i = h_i - c_i$ for all $i \in \mathcal{I}$. Therefore $\mathbf{h} \neq \mathbf{c}$ if and only if $\tilde{\mathbf{h}} \neq \mathbf{0}$. We conclude that

$$\mathbf{y} \in B(\mathbf{c}) \text{ if and only if } \tilde{\mathbf{y}} \in B(\mathbf{0})$$

This completes the proof of the theorem for the case of SP decoding. It is trivial to see that this proof generalizes to the case of optional early exit of the iterative loop on successful completion of a syndrome check. ■

V. APPLICATION: NONBINARY CODES MAPPED TO PSK MODULATION

While this theorem may be shown to apply to other coded modulation systems such as nonbinary coded orthogonal modulation over memoryless channels and nonbinary coding over the discrete memoryless q -ary symmetric channel, we focus in this paper on the practical application of nonbinary codes mapped directly to PSK symbols and transmitted over a memoryless channel. Here $\Sigma = \mathbb{C}$, and denoting the ring elements by $\mathfrak{R} = \{a_0, a_1, \dots, a_{q-1}\}$, the modulation mapping may be written without loss of generality as

$$M : \mathfrak{R} \mapsto \mathbb{C}$$

such that

$$M(a_k) = \exp\left(\frac{i2\pi k}{q}\right) \quad (23)$$

for $k = 0, 1, \dots, q-1$ (here $i = \sqrt{-1}$). Here (15), together with the rotational symmetry of the q -ary PSK constellation, motivates us to define, for every $\beta = a_k \in \mathfrak{R}$,

$$\tau_\beta(x) = \exp\left(\frac{-i2\pi k}{q}\right) \cdot x \quad \forall x \in \mathbb{C} \quad (24)$$

Next, we also impose the condition that \mathfrak{R} under addition is a cyclic group. To see why we impose this condition, let $\alpha = a_k \in \mathfrak{R}$ and $\beta = a_l \in \mathfrak{R}$. By the symmetry condition we must have

$$p(y_i | \alpha + \beta) = p(\tau_{\alpha+\beta}(y_i) | 0)$$

and also

$$p(y_i | \alpha + \beta) = p(\tau_\beta(y_i) | \alpha) = p(\tau_\alpha(\tau_\beta(y_i)) | 0)$$

In order to equate these two expressions, we impose the condition $\tau_{\alpha+\beta}(x) = \tau_\alpha(\tau_\beta(x))$ for all $x \in \mathbb{C}$, $\alpha, \beta \in \mathfrak{R}$. Letting $\alpha + \beta = a_p \in \mathfrak{R}$, and using (24) yields

$$\exp\left(\frac{-i2\pi k}{q}\right) \cdot \exp\left(\frac{-i2\pi l}{q}\right) = \exp\left(\frac{-i2\pi p}{q}\right)$$

and thus $p \equiv k + l \pmod{q}$.

Therefore, we must have

$$a_k + a_l = a_{(k+l) \bmod q} \quad (25)$$

for all $a_k, a_l \in \mathfrak{R}$. This implies that \mathfrak{R} , under addition, is a cyclic group.

It is easy to check that the condition that \mathfrak{R} under addition is cyclic, encapsulated by (25), along with the modulation mapping (23), satisfies the symmetry condition, where the appropriate mappings τ_β are given by (24). This means that codeword-independent performance is guaranteed for such systems using nonbinary codes with PSK modulation. This applies to AWGN, flat fading wireless channels, and OFDM systems transmitting over frequency selective channels with sufficiently long cyclic prefix.

ACKNOWLEDGMENT

The author would like to thank M. Greferath and V. Skachek for providing helpful comments which improved the presentation of this paper. This work was supported by the Claude Shannon Institute, Dublin, Ireland (Science Foundation Ireland Grant 06/MI/006), the University of Bologna (ESRF-ISA) and the EC-IST Optimix project (IST-214625).

REFERENCES

- [1] R. G. Gallager, "Low-density parity-check codes," *IRE Transactions on Information Theory*, vol. IT-8, no. 1, pp. 21–28, January 1962.
- [2] A. Bennatan and D. Burshtein, "Design and analysis of nonbinary LDPC codes for arbitrary discrete-memoryless channels," *IEEE Transactions on Information Theory*, vol. 52, issue. 2, pp. 549–583, February 2006.
- [3] J. Feldman, M. J. Wainwright and D. R. Karger, "Using linear programming to decode binary linear codes," *IEEE Transactions on Information Theory*, vol. 51, no. 3, pp. 954–972, March 2005.
- [4] M. F. Flanagan, V. Skachek, E. Byrne and M. Greferath, "Linear-programming decoding of non-binary linear codes," *Proc. 7th International Conference on Source and Channel Coding, SCC 2008*, Ulm, Germany, 14–16 January 2008. Available online at <http://arxiv.org/abs/0707.4360>.
- [5] G. D. Forney, Jr., "Geometrically uniform codes," *IEEE Transactions on Information Theory*, vol. 37, issue. 5, pp. 1241–1260, September 1991.
- [6] D. Sridhara and T. E. Fuja, "LDPC codes over rings for PSK modulation," *IEEE Transactions on Information Theory*, vol. 51, no. 9, pp. 3209–3220, September 2005.
- [7] T. Richardson and R. E. Urbanke, "On the capacity of LDPC codes under message-passing decoding," *IEEE Transactions on Information Theory*, vol. 51, no. 9, pp. 3209–3220, September 2005.