Symbol Message Passing Decoding of LDPC Codes for Orthogonal Modulations

Emna Ben Yacoub[‡], Balazs Matuz[†]
[‡]Institute for Communications Engineering, Technical University of Munich, Germany
[†]Institute of Communications and Navigation, German Aerospace Center (DLR), Germany
Email: emna.ben-yacoub@tum.de, balazs.matuz@dlr.de

***Abstract*—A simple decoder for q-ary low-density parity-check codes is studied, termed symbol message passing. The decoder passes hard decisions from a q-ary alphabet. For orthogonal modulations over the additive white Gaussian channel for which the modulation order and the field order q are equal, it is shown that the extrinsic messages can be modelled as observations of a q-ary symmetric channel, allowing to work out density evolution equations. A stability analysis is provided which emphasizes the influence of degree-3 variable nodes. Simulation results show performance gains for increasing q w.r.t. binary low-density parity-check codes with bit-interleaved coded modulation, and potential savings in decoding complexity.**

I. Introduction

Non-binary low-density parity-check (LDPC) codes have been proposed for various applications to improve the performance of their binary counterparts [1], [2]. Several decoding algorithms have been studied in the literature to decrease the complexity of the non-binary operations in the decoder [3], [4], [5], [6]. Amongst others, Hadamard-Walsh transform based decoders facilitate the computation of the check node (CN) operations [6] while extended min-sum decoders consider only a subset of the q reliabilities of each symbol [3].

Recently, a symbol message passing (SMP) decoder for non-binary LDPC codes over the q-ary symmetric channel (qSC) was proposed [7]. Messages in the decoder consist of the most reliable symbol only. This is similar to an extended min-sum decoder where only the most reliable value of a q-ary symbol is considered. However, instead of passing reliabilities, hard decisions are propagated in SMP decoders. The simple decoding operations let SMP decoders be used for applications requiring high throughput/low decoding complexity, rather than capacity approaching performance. This stands in contrast to the original purpose of non-binary LDPC codes and decoders.

This work extends the results of [7] on qSCs to additive white Gaussian noise (AWGN) channels with orthogonal modulations where the field order q and the modulation order are equal. This makes non-binary LDPC codes a natural choice since each q-ary modulation symbol is in one-to-one correspondence with a q-ary code symbol. Our aim is to show that non-binary LDPC codes with low-complexity decoding algorithms are favorable for certain coded-modulation scenarios. To this end, we provide a density evolution (DE) analysis for orthogonal modulations which finds good degree distributions for unstructured LDPC code ensembles. This is complemented by a stability analysis which shows that not only degree-2, but also degree-3 variable nodes (VNs) must be handled with care. The simple decoding algorithm thresholds show a gap of around 2.1 dB with respect to channel capacity. However, numerical simulation results show that q-ary LDPC codes with SMP decoders outperform binary LDPC codes in a bit-interleaved coded modulation (BICM) setting for increasing q, with potentially lower decoding complexity.

II. Preliminaries

A. System Model

Consider LDPC codes over $\mathbb{F}_q = \{0, 1, \alpha, \dots, \alpha^{q-2}\}$ with $q = 2^m$, m a positive integer and α a primitive element of $\mathbb{F}_q$. We denote a length-N codeword as $\boldsymbol{c} = (c_1, c_2, \dots, c_N)$, with $c_i \in \mathbb{F}_q$. We consider one-to-one mappings between codeword symbols c_i and orthogonal modulation symbols $\boldsymbol{\chi}(c_i)$. Each modulation symbol is represented as a length-q vector $\boldsymbol{\chi}(c_i) = \big(\chi_0(c_i), \chi_1(c_i), \dots, \chi_{\alpha^{q-2}}(c_i)\big)$ where for convenience we index its entries by elements of $\mathbb{F}_q$ rather than by integers $1, 2, \dots, q$. For orthogonal modulations $\forall a, a' \in \mathbb{F}_q$ we have

$$\langle \boldsymbol{\chi}(a), \boldsymbol{\chi}(a') \rangle = \begin{cases} 1 & a = a' \\ 0 & \text{otherwise} \end{cases}$$

where $\langle \cdot, \cdot \rangle$ is the inner product. Without loss of generality we consider pulse position modulation (PPM) for which $\forall a \in \mathbb{F}_q$

$$\chi_a(c_i) = \begin{cases} 1 & a = c_i \\ 0 & \text{otherwise.} \end{cases}$$

For transmission over an AWGN channel with input alphabet $\mathcal{X} = \big\{\boldsymbol{\chi}(0), \boldsymbol{\chi}(1), \dots, \boldsymbol{\chi}(\alpha^{q-2})\big\}$, the observation of the ith modulated symbol is

$$\boldsymbol{y}_i = \boldsymbol{\chi}(c_i) + \boldsymbol{n}_i$$

where $\boldsymbol{n}_i = (n_{i,0}, n_{i,1}, \dots, n_{i,\alpha^{q-2}})$ is the length-q noise vector sampled from q independent and identically distributed Gaussian random variables (RVs) with zero-mean and variance σ_{N}^2. For ease of notation, we will drop the modulation symbol index i whenever possible. For $a \in \mathbb{F}_q$ the likelihood $p_{\boldsymbol{Y}|A}(\boldsymbol{y}|a)$ can be written as

$$p(\boldsymbol{y}|a) = \left(\frac{1}{\sqrt{2\pi\sigma_{\mathrm{N}}^2}}\right)^q \exp\left(-\frac{||\boldsymbol{y}-\boldsymbol{\chi}(a)||^2}{2\sigma_{\mathrm{N}}^2}\right) \quad (1)$$
$$\propto \exp\left(-\frac{1}{\sigma_{\mathrm{N}}^2}\langle \boldsymbol{y}, \boldsymbol{\chi}(a)\rangle\right).$$

Let E_{b} denote the energy per information bit, E_{s} the energy per modulation symbol and N_0 is the one-sided noise power spectral density. Then, we have

$$\frac{E_{\mathsf{b}}}{N_0} = \frac{1}{Rm}\frac{E_{\mathrm{s}}}{N_0} = \frac{1}{Rm}\frac{1}{2\sigma_{\mathrm{N}}^2}.$$

B. Decoder messages

The messages in an iterative decoder can be modelled as an observation from an *extrinsic* channel [8]. For the AWGN channel with q-ary orthogonal modulations and SMP decoding of q-ary LDPC codes, the extrinsic channel is a qSC. Details follow in Section IV. The transition probabilities of a qSC with error probability ϵ are

$$P(w|a) = \begin{cases} 1-\epsilon & \text{if } w = a \\ \frac{\epsilon}{q-1} & \text{otherwise.} \end{cases}$$

For convenience we work with log-likelihood values (L-values) $L_a(w) = \log\left(P(w|a)\right)$ $a \in \mathbb{F}_q$. L-values can be compactly expressed as length-q log-likelihood vectors ($\boldsymbol{L}$-vectors) with

$$\boldsymbol{L}(w) = \left(L_0(w), L_1(w), \ldots, L_{\alpha^{q-2}}(w)\right).$$

Lemma 1. *Suppose the $w^{(i)}$, $i = 1, 2, \ldots, d$, are observations of a qSC with $1-\epsilon > \frac{\epsilon}{q-1}$. When summing d $\boldsymbol{L}$-vectors $\boldsymbol{L}\left(w^{(i)}\right)$, the elements of the sum with indices $\mathcal{I} = \bigcup_{i=1}^{d} w^{(i)}$, where $|\mathcal{I}| \le \min(d, q)$, all have values greater than $d \log \frac{\epsilon}{q-1}$ and thus contain the maximum value of the sum.*

Proof. Observe that each $\boldsymbol{L}\left(w^{(i)}\right)$ has a single maximum with index $a = w^{(i)}$ and that all other entries are $\log \frac{\epsilon}{q-1}$. $\square$

Similarly, let the channel message be represented by a length-q $\boldsymbol{L}$-vector

$$\boldsymbol{L}(\boldsymbol{y}) = \left(L_0(\boldsymbol{y}), L_1(\boldsymbol{y}), \ldots, L_{\alpha^{q-2}}(\boldsymbol{y})\right) \quad (2)$$

with $L_a(\boldsymbol{y}) = \log\left(p(\boldsymbol{y}|a)\right)$. While the transition probability densities $p(\boldsymbol{y}|a)$ of the communication channel are given in (1), the transition probabilities of the extrinsic channel are in general unknown, but accurate estimates can be obtained via DE analysis [9].

C. Non-binary LDPC Codes

Non-binary LDPC codes can be defined by an $M \times N$ sparse parity-check matrix $\boldsymbol{H} = [h_{i,j}]$ with entries in $\mathbb{F}_q$. The parity-check matrix can be represented by a Tanner graph with N VNs corresponding to codeword symbols and M CNs corresponding to parity checks. Each edge connecting $\mathtt{v}$ and $\mathtt{c}$ is labeled by a non-zero element $h_{\mathtt{v},\mathtt{c}}$ of $\boldsymbol{H}$. The sets $\mathcal{N}(\mathtt{v})$ and $\mathcal{N}(\mathtt{c})$ denote the neighbors of VN $\mathtt{v}$ and CN $\mathtt{c}$, respectively. The degree of a VN $\mathtt{v}$ is the cardinality of the set $\mathcal{N}(\mathtt{v})$. Similarly, the degree of a CN $\mathtt{c}$ is the cardinality of the set $\mathcal{N}(\mathtt{c})$. The VN edge-oriented degree distribution polynomial is $\lambda(x) = \sum_{i=1}^{d_{\mathtt{v}}} \lambda_i x^{i-1}$ where λ_i is the fraction of edges incident to VNs with degree i and $d_{\mathtt{v}}$ is the maximum VN degree. Similarly, the CN edge-oriented degree distribution polynomial is $\rho(x) = \sum_{i=2}^{d_{\mathtt{c}}} \rho_i x^{i-1}$ where ρ_i is the fraction of edges incident to CNs with degree i and $d_{\mathtt{c}}$ is the maximum CN degree. An unstructured irregular LDPC code ensemble $\mathscr{C}_{\lambda,\rho}^{q,N}$ is the set of all q-ary LDPC codes with block length N and degree distribution polynomials $\lambda(x)$ and $\rho(x)$.

III. Symbol Message Passing Algorithm

Let $m_{\mathtt{c}\to\mathtt{v}}^{(\ell)}$ be the message sent from CN $\mathtt{c}$ to its neighboring VN $\mathtt{v}$ at the ℓth iteration and $m_{\mathtt{v}\to\mathtt{c}}^{(\ell)}$ the message sent from VN $\mathtt{v}$ to CN $\mathtt{c}$ at the ℓth iteration. All exchanged messages between the CNs and VNs are from a q-ary alphabet. Decoding proceeds as follows.

1) Initialization: Each VN computes the channel $\boldsymbol{L}$-vector defined in (2) and sends the symbol with the highest L-value. Since

$$L_a(\boldsymbol{y}) = \frac{y_a}{\sigma_{\mathrm{N}}^2} - \frac{q}{2}\log(2\pi\sigma_{\mathrm{N}}^2) - \frac{\|\boldsymbol{y}\|^2 + 1}{2\sigma_{\mathrm{N}}^2} \quad \forall a \in \mathbb{F}_q$$

finding the maximum of the length-q vector $\boldsymbol{L}(\boldsymbol{y})$ is equivalent to finding the maximum of $\boldsymbol{y}$. Hence, we have

$$m_{\mathtt{v}\to\mathtt{c}}^{(0)} = \underset{a \in \mathbb{F}_q}{\operatorname{argmax}}\, L_a(\boldsymbol{y}) = \underset{a \in \mathbb{F}_q}{\operatorname{argmax}}\, y_a. \quad (3)$$

The complexity of the initialization step scales as $\mathcal{O}(Nq)$. The performed operation is finding a maximum.

2) CN update: At the ℓth iteration, CN $\mathtt{c}$ sends to its neighboring VN $\mathtt{v}$ the following message:

$$m_{\mathtt{c}\to\mathtt{v}}^{(\ell)} = -h_{\mathtt{c},\mathtt{v}}^{-1} \sum_{\mathtt{v}' \in \mathcal{N}(\mathtt{c})\setminus\mathtt{v}} h_{\mathtt{v},\mathtt{c}'} m_{\mathtt{v}'\to\mathtt{c}}^{(\ell-1)}$$

where $h_{\mathtt{c},\mathtt{v}}$ is the respective parity-check matrix element and $h_{\mathtt{c},\mathtt{v}}^{-1}$ is its inverse in $\mathbb{F}_q$. From [7] the CN operation can be implemented with $2d_{\mathtt{c}} - 1$ q-ary additions and $2d_{\mathtt{c}}$ q-ary multiplications. If q-ary additions/multiplications are implemented using elementary operations the complexity may depend on q. For instance, the sum of two q-ary symbols can be performed by $\log_2 q$ binary XOR operations. Thus, the complexity scales as $\mathcal{O}(M d_{\mathtt{c}} f(q))$, where $f(\cdot)$ is an implementation dependent cost.

3) VN update: Each VN performs the following operations

$$m_{\mathtt{v}\to\mathtt{c}}^{(\ell)} = \underset{a \in \mathbb{F}_q}{\operatorname{argmax}}\, L_{\mathrm{ex},a}^{(\ell)}$$

where

$$\begin{aligned} \boldsymbol{L}_{\mathrm{ex}}^{(\ell)} &= \left[L_{\mathrm{ex},0}^{(\ell)}, L_{\mathrm{ex},1}^{(\ell)}, \ldots, L_{\mathrm{ex},\alpha^{q-2}}^{(\ell)}\right] \quad (4) \\ &= \boldsymbol{L}(\boldsymbol{y}) + \sum_{\mathtt{c}' \in \mathcal{N}(\mathtt{v})\setminus\mathtt{c}} \boldsymbol{L}\left(m_{\mathtt{c}'\to\mathtt{v}}^{(\ell)}\right). \end{aligned}$$

The complexity of the VN operation scales as $\mathcal{O}(Nd_{\mathrm{v}})$: as shown in [7] all d_{v} extrinsic messages can be computed efficiently from the sum of *all* incoming messages $\sum_{\mathtt{c}'\in\mathcal{N}(\mathtt{v})}\boldsymbol{L}\left(m^{(\ell)}_{\mathtt{c}'\to\mathtt{v}}\right)$ and $\boldsymbol{L}\left(\boldsymbol{y}\right)$, denoted by $\boldsymbol{L}^{(\ell)}_{\text{tot}}$. Let the entry with index a be the maximum of $\boldsymbol{L}\left(\boldsymbol{y}\right)$ computed in (3).[1] By Lemma 1 the largest values of $\boldsymbol{L}^{(\ell)}_{\text{tot}}$ will be in $\mathcal{I}\cup a$, where $|\mathcal{I}\cup a|\leq\min(d_{\mathrm{v}}+1,q)\leq d_{\mathrm{v}}+1$. This step requires $\mathcal{O}(d_{\mathrm{v}})$ additions of floats. The identification of the (two) largest values of $\boldsymbol{L}^{(\ell)}_{\text{tot}}$ requires d_{v} steps. Then, the extrinsic messages and their maximum can be obtained from $\boldsymbol{L}^{(\ell)}_{\text{tot}}$ with d_{v} additional operations (subtractions, comparisons) and we have an overall complexity scaling of $\mathcal{O}(Nd_{\mathrm{v}})$.

4) Hard decision: Each VN computes an estimation of its codeword symbol as follows

$$\hat{c}^{(\ell)}_{\mathtt{v}}=\underset{a\in\mathbb{F}_q}{\operatorname{argmax}}\left(L_a(\boldsymbol{y})+\sum_{\mathtt{c}'\in\mathcal{N}(\mathtt{v})}L_a(m^{(\ell)}_{\mathtt{c}'\to\mathtt{v}})\right).$$

IV. Density Evolution Analysis

We discuss DE analysis for SMP for non-binary irregular LDPC code ensembles. Due to symmetry, we can assume the all-zero codeword was transmitted. Let $p^{(\ell)}_a$ ($s^{(\ell)}_a$) be the probability that a variable to check (check to variable) message takes value $a\in\mathbb{F}_q$ at the ℓth iteration. Let $\ell_{\max}$ be the maximum number of iterations. In the limit of $N\to\infty$, the evolution of the message distributions is as follows.

1) Initialization: Define the random vector

$$\boldsymbol{Z}_a=Y_a\mathbf{1}_{q-1}-\boldsymbol{Y}_{[a]} \tag{5}$$

for $a\in\mathbb{F}_q$, with $\boldsymbol{Y}_{[a]}$ being the random vector $\boldsymbol{Y}$ of channel observations without the entry Y_a and $\mathbf{1}_{q-1}$ the length-$(q-1)$ all-one vector. It is easy to check that $\forall a\in\mathbb{F}_q$

$$p^{(0)}_a=\Pr\left\{\boldsymbol{Z}_a>\mathbf{0}\right\}. \tag{6}$$

Conditioned on the transmission of the all-zero codeword, we have $\boldsymbol{Y}$ is a Gaussian random vector with mean $\boldsymbol{\mu}_{\boldsymbol{Y}}=(1,0,\ldots,0)$ and covariance matrix $\boldsymbol{\Sigma}_{\boldsymbol{Y}}=\sigma^2_{\mathrm{N}}\boldsymbol{I}_q$, where $\boldsymbol{I}_q$ is the size q identity matrix. Thus, $\boldsymbol{Z}_a$ is a Gaussian random vector with mean

$$\boldsymbol{\mu}_{\boldsymbol{Z}_a}=\begin{cases}\mathbf{1}_{q-1} & a=0\\ (-1,0,\ldots,0) & a\in\mathbb{F}_q\setminus\{0\}\end{cases}$$

and covariance matrix $\boldsymbol{\Sigma}_{\boldsymbol{Z}_a}$ with entries

$$(\boldsymbol{\Sigma}_{\boldsymbol{Z}_a})_{i,j}=\begin{cases}2\sigma^2_{\mathrm{N}} & i=j\\ \sigma^2_{\mathrm{N}} & \text{otherwise.}\end{cases}$$

The parameters of $\boldsymbol{Z}_a$ $\forall a\in\mathbb{F}_q\setminus\{0\}$ do not depend on a and thus take the same value. Therefore, $\forall a\in\mathbb{F}_q\setminus\{0\}$ we have

$$p^{(0)}_a=\frac{1-p^{(0)}_0}{q-1}$$

where

$$p^{(0)}_0=\Pr\left\{\boldsymbol{Z}_0>\mathbf{0}\right\}$$

from (6). Observe that $p^{(0)}_0$ and $p^{(0)}_a$ with $a\in\mathbb{F}_q\setminus\{0\}$ are transition probabilities of a qSC where $1-p^{(0)}_0$ is the channel error probability formerly denoted by ϵ.

2) Evolution of densities for $\ell=1,2,\ldots,\ell_{max}$: For the **check to variable update** we have

$$s^{(\ell)}_0=\frac{1}{q}\left[1+(q-1)\rho\left(\frac{q\cdot p^{(\ell-1)}_0-1}{q-1}\right)\right]$$

and $\forall a\in\mathbb{F}_q\setminus\{0\}$

$$s^{(\ell)}_a=\frac{1-s^{(\ell)}_0}{q-1}.$$

Again, the extrinsic channel is a qSC with error probability $1-s^{(\ell)}_0$.

For the **variable to check update** we introduce the random vector $\boldsymbol{F}^{(\ell)}=\left(F^{(\ell)}_0,\ldots,F^{(\ell)}_{\alpha^{q-2}}\right)$, where $F^{(\ell)}_a$ denotes the RV associated to the number of incoming CN messages to a degree-d VN that takes value $a\in\mathbb{F}_q$ at the ℓth iteration, and $f^{(\ell)}_a$ is its realization. The entries of $\boldsymbol{L}^{(\ell)}_{\text{ex}}$ in (4) are

$$\begin{aligned}L^{(\ell)}_{\text{ex},a}&=\frac{y_a}{\sigma^2_{\mathrm{N}}}+\mathsf{D}^{(\ell)}f^{(\ell)}_a+K\\ \mathsf{D}^{(\ell)}&=\log(s^{(\ell)}_0)-\log((1-s^{(\ell)}_0)/(q-1))\\ K&=-\frac{q}{2}\log(2\pi\sigma^2_{\mathrm{N}})-\frac{\|\boldsymbol{y}\|^2+1}{2\sigma^2_{\mathrm{N}}}\\ &\quad+(d-1)\log((1-s^{(\ell)}_0)/(q-1)).\end{aligned} \tag{7}$$

K in (7) is independent of a and can be ignored when computing $\boldsymbol{L}^{(\ell)}_{\text{ex}}$. We obtain (8) $\forall a\in\mathbb{F}_q$ where $\boldsymbol{f}^{(\ell)}_{[a]}$ is the vector $\boldsymbol{f}^{(\ell)}$ without its entry $f^{(\ell)}_a$, $\boldsymbol{Z}_a$ is defined in (5) and the sum is over integer vectors $\boldsymbol{f}^{(\ell)}$ for which it holds $0\leq f^{(\ell)}_u\leq d-1\,\forall u\in\mathbb{F}_q$ and $\sum_{u\in\mathbb{F}_q}f^{(\ell)}_u=d-1$ and

$$\Pr\{\boldsymbol{F}^{(\ell)}=\boldsymbol{f}^{(\ell)}\}=\binom{d-1}{f^{(\ell)}_0,\ldots,f^{(\ell)}_{\alpha^{q-2}}}(s^{(\ell)}_0)^{f^{(\ell)}_0}\times\left(\frac{1-s^{(\ell)}_0}{q-1}\right)^{d-1-f^{(\ell)}_0}.$$

The ensemble iterative decoding threshold $(E_{\mathsf{b}}/N_0)^\star$ is defined as the minimum E_{b}/N_0 for which $p^{(\ell)}_0\to 1$ as $\ell\to\infty$.

V. Stability Condition

We define $\bar{p}^{(\ell)}_0=1-p^{(\ell)}_0$ and $\bar{s}^{(\ell)}_0=1-s^{(\ell)}_0$. The stability analysis examines the convergence of the probability $\bar{p}^{(\ell)}_0$ to

[1]For an unquantized AWGN channel $\boldsymbol{L}\left(\boldsymbol{y}\right)$ has a unique maximum with probability one.

$$
\begin{aligned}
p_a^{(\ell)} &= \sum_d \lambda_d \sum_{\boldsymbol{f}^{(\ell)}} \Pr\{\boldsymbol{F}^{(\ell)} = \boldsymbol{f}^{(\ell)}\} \Pr\left\{ \underset{u\in\mathbb{F}_q}{\operatorname{argmax}} \, L_{\mathrm{ex},a}^{(\ell)} = a \middle| \boldsymbol{f}^{(\ell)} \right\} \\
&= \sum_d \lambda_d \sum_{\boldsymbol{f}^{(\ell)}} \Pr\{\boldsymbol{F}^{(\ell)} = \boldsymbol{f}^{(\ell)}\} \Pr\left\{ \boldsymbol{Z}_a > \sigma_{\mathrm{N}}^2 \mathsf{D}^{(\ell)} \left(\boldsymbol{f}_{[a]}^{(\ell)} - f_a^{(\ell)} \mathbf{1}_{q-1} \right) \right\}
\end{aligned} \tag{8}
$$

zero under the assumption that it is close to the fixed point $\bar{p}_0^\star = 0$. Note that $\bar{s}_0^{(\ell)} \to 0$ as $\bar{p}_0^{(\ell)} \to 0$. Thus, $\mathsf{D}^{(\ell)} \to \infty$ and

$$
\begin{aligned}
\bar{p}_0^{(\ell)} = & \sum_d \lambda_d \sum_{a\in\mathbb{F}_q} \left[\sum_{\boldsymbol{f}^{(\ell)}\in\mathcal{F}_{1,a}} \Pr\{\boldsymbol{F}^{(\ell)} = \boldsymbol{f}^{(\ell)}\} \right. \\
& \left. + \sum_{\boldsymbol{f}^{(\ell)}\in\mathcal{F}_{2,a}} \Pr\{\boldsymbol{F}^{(\ell)} = \boldsymbol{f}^{(\ell)}\} \Pr\{\underset{e\in\mathcal{S}}{\operatorname{argmax}} \, Y_e = a\} \right]
\end{aligned}
$$

where $\mathcal{F}_{1,a}$ is the set of all integer vectors $\boldsymbol{f}^{(\ell)}$ for which it holds $\sum_{u\in\mathbb{F}_q} f_u^{(\ell)} = d-1$ and $f_a^{(\ell)} > f_u^{(\ell)} \geq 0 \, \forall u \in \mathbb{F}_q \setminus \{a\}$. $\mathcal{F}_{2,a}$ is the set of all integer vectors $\boldsymbol{f}^{(\ell)}$ for which it holds $\sum_{u\in\mathbb{F}_q} f_u^{(\ell)} = d-1$ and $f_a^{(\ell)} > f_u^{(\ell)} \geq 0 \, \forall u \in \mathbb{F}_q \setminus \mathcal{S}_a$ where

$$
\mathcal{S}_a = \{b \in \mathbb{F}_q | f_b^{(\ell)} = f_a^{(\ell)}\}
$$

and $|\mathcal{S}_a| > 1$. Recall that for any $a \in \mathbb{F}_q \setminus \{0\}$

$$
\Pr\{\boldsymbol{F}^{(\ell)} = \boldsymbol{f}^{(\ell)}\} = \binom{d-1}{f_0^{(\ell)}, \dots, f_{\alpha^{q-2}}^{(\ell)}} (1 - \bar{s}_0^{(\ell)})^{f_0^{(\ell)}} \times \left(\frac{\bar{s}_0^{(\ell)}}{q-1} \right)^{d-1-f_0^{(\ell)}}.
$$

We obtain

$$
\lim_{\bar{s}_0^{(\ell)} \to 0} \frac{\mathrm{d}\bar{p}_0^{(\ell)}}{\mathrm{d}\bar{s}_0^{(\ell)}} = \lambda_2 + 2\lambda_3 Q \left(\frac{1}{\sqrt{2\sigma_{\mathrm{N}}^2}} \right). \tag{9}
$$

Furthermore, we have

$$
\bar{s}_0^{(\ell)} = \frac{q-1}{q} \left[1 - \rho \left(1 - \frac{q\bar{p}_0^{(\ell-1)}}{q-1} \right) \right]
$$

and

$$
\lim_{\bar{p}_0^{(\ell-1)} \to 0} \frac{\mathrm{d}\bar{s}_0^{(\ell)}}{\bar{p}_0^{(\ell-1)}} = \rho'(1). \tag{10}
$$

The first order Taylor expansions via (9), (10) yield

$$
\bar{p}_0^{(\ell)} = \rho'(1) \left[\lambda_2 + 2\lambda_3 Q \left(\frac{1}{\sqrt{2\sigma_{\mathrm{N}}^2}} \right) \right] \bar{p}_0^{(\ell-1)}.
$$

The stability condition is fulfilled if and only if

$$
\rho'(1) \left[\lambda_2 + 2\lambda_3 Q \left(\frac{1}{\sqrt{2\sigma_{\mathrm{N}}^2}} \right) \right] < 1.
$$

Remark 1. The fraction of edges connected to degree 2 *and* 3 VNs impacts the stability condition for SMP decoding. Thus, certain degree distributions optimized for unquantized belief propagation (see, e.g., [10]) might be unsuitable for SMP due to their large number of degree 2 and 3 VNs.

VI. Numerical Results

A. Iterative Decoding Thresholds

The DE analysis in Section IV suggests an optimization algorithm to find rate $R = 1/2$ irregular LDPC ensembles with 'good' thresholds for $q \in \{8, 16, 32\}$. We restrict the maximum VN degree to 12 and perform two optimizations: one without further constraints and one with constraints on the degree two and three VNs. Threshold results are depicted in Table I and show a gap of at least 2.1 dB with respect to the Shannon limit for various q. Thresholds of q-ary LDPC codes under full belief propagation (BP) decoding in [10] show only gaps of 0.2 dB, i.e., the simple SMP decoder yields a loss of around 1.9 dB. Interestingly, for binary LDPC codes with orthogonal modulations and BICM (no iterative detection) the gap to coded modulation capacity is comparable or even larger. For instance, for $q = 16$ the gap is 1.8 dB [10, Fig. 1].

B. Monte Carlo Simulations

We designed three codes with $q \in \{8, 16, 32\}$, $N = 10000$ (in $\mathbb{F}_q$ symbols), and $R = 1/2$ based on the constraint degree distribution pairs from Table I. Figure 1 shows the frame error rate (FER) versus E_{b}/N_0 of q-ary PPM allowing a maximum of 50 decoding iterations. Observe that the waterfall performance is well predicted by the DE analysis. In addition, we provide the performance of three $R = 1/2$ binary accumulate-repeat-4-jagged-accumulate (AR4JA) LDPC codes assuming a BICM setting and q-ary PPM for $q \in \{8, 16, 32\}$. The AR4JA protograph was taken from [11] and expanded to obtain block lengths (in bits) of $N \log_2 q$. For $q \geq 16$ the performance of the non-binary codes under SMP decoding are competitive and for $q = 32$ they outperform the AR4JA codes with BICM by almost 0.2 dB.

C. Complexity

Despite the gap to capacity in Table I, SMP decoding might be a good choice when low-complexity decoding is targeted. First, a comparison of the algorithmic complexity of the SMP decoder (from Section III) and a binary LDPC decoder with BICM is given in Table II. For the binary decoder, the initialization step requires computing symbol-wise probabilities, followed by a marginalization to obtain bit-wise log-likelihood ratios (LLRs). The CN operations in the binary decoder follow the approximate min* rule [12]. The VN operations consist of summing up LLRs. Table II indicates that the algorithmic complexity of SMP is competitive with binary BP, but a fair comparison is difficult due to the different types of operations. E.g., the approximate min* rule and the SMP CN operations can be implemented by look-up tables. Then, an elementary

TABLE I

THRESHOLDS $(E_b/N_0)^\star$ OF $R = 1/2$ LDPC CODE ENSEMBLES UNDER SMP. SHANNON LIMIT $(E_b/N_0)_{Sh}$ AS A REFERENCE. ENSEMBLES WITH CONSTRAINTS ON LOW-DEGREE NODES ARE MARKED WITH •.

q	$\lambda(x)$	$\rho(x)$		$(E_b/N_0)^\star$ [dB]	$(E_b/N_0)_{Sh}$ [dB]
4	$0.0187x + 0.5597x^2 + 0.003x^3 + 0.4186x^{11}$	$0.3358x^7 + 0.6642x^8$		3.22	1.06
	$0.3699x^2 + 0.2799x^3 + 0.3502x^{11}$	$0.0084x^7 + 0.9916x^8$	•	3.40	
8	$0.0465x + 0.5735x^2 + 0.38x^{11}$	$0.859x^7 + 0.141x^8$		2.19	0.08
	$0.4407x^2 + 0.2652x^3 + 0.2941x^{11}$	$0.5576x^7 + 0.4424x^8$	•	2.39	
16	$0.0595x + 0.5868x^2 + 0.3537x^{11}$	$0.1351x^6 + 0.8649x^7$		1.63	-0.47
	$0.5199x^2 + 0.1436x^3 + 0.3365x^{11}$	$0.5407x^7 + 0.4593x^8$	•	1.82	
32	$0.0582x + 0.6141x^2 + 0.3277x^{11}$	$0.311x^6 + 0.689x^7$		1.32	-0.80
	$0.55x^2 + 0.1424x^3 + 0.3076x^{11}$	$0.8045x^7 + 0.1955x^8$	•	1.48	

TABLE II

COMPLEXITY SCALING OF ALGORITHMIC OPERATIONS.

	SMP	BP with BICM
Init	$\mathcal{O}(Nq)$ maximization	$\mathcal{O}(Nq\log_2 q)$ sum of floats
CN	$\mathcal{O}(Md_c f(q))$ elementary operations	$\mathcal{O}(Md_c \log_2 q)$ box-plus/multiplications
VN	$\mathcal{O}(Nd_v)$ addition of floats/maximization	$\mathcal{O}(Nd_v \log_2 q)$ addition of floats

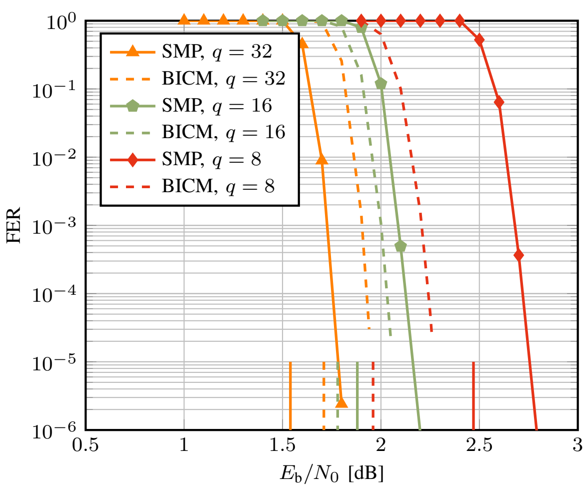

Fig. 1. FER versus E_b/N_0 for SMP and BP with BICM. Respective thresholds are indicated by vertical lines.

operation is a look-up with $f(q) = 1$ and complexity is reduced by a factor of $\log_2 q$ w.r.t. the binary decoder. Other implementations may change the picture. Second, an important figure for implementation is the data flow in the decoder [13]. For SMP we need $\log_2 q$ bits to represent a symbol, for binary BP typically 4 to 5 bits to represent an LLR. Since the binary Tanner graph has $\log_2 q$ times more nodes the data flow of the SMP decoder will be lower by a factor of 4 to 5 (for the same average node degrees). Overall, the algorithmic complexity/data flow of an SMP decoder is highly competitive w.r.t. that of a binary decoder with BICM. However, only a hardware implementation will give final insights.

VII. CONCLUSIONS

We investigate SMP decoding of q-ary LDPC codes on AWGN channels with q-ary orthogonal modulations. By showing that the extrinsic messages are observations of a qSC we apply DE to derive thresholds of unstructured code ensembles. A stability analysis suggests that not only degree two, but also degree three VNs impact stability. Thresholds of optimized irregular code ensembles reveal a gap of 2.1 dB w.r.t. the Shannon limit. Despite this gap, a comparison with binary LDPC codes and BICM shows performance gains for increasing q with possible advantages in complexity of SMP. An open question is whether SMP decoders can be efficiently implemented in hardware.

REFERENCES

[1] M. Davey and D. MacKay, "Low density parity check codes over GF(q)," *IEEE Communications Letters*, vol. 2, pp. 70–71, 1996.

[2] *Short block length LDPC codes for TC synchronization and channel coding*, Orange Book, Issue 1, Consultative Committee for Space Data Systems (CCSDS) Experimental specification 231.1-O-1, Sep. 2015.

[3] D. Declercq and M. Fossorier, "Decoding algorithms for nonbinary LDPC codes over GF(q)," *IEEE Trans. Commun.*, vol. 55, no. 4, pp. 633–643, 2007.

[4] V. Savin, "Min-max decoding for non binary LDPC codes," in *Int. Symp. Inf. Theory*, Toronto, Canada, Jul. 2008, pp. 960–964.

[5] E. Boutillon and L. Conde-Canencia, "Simplified check node processing in nonbinary LDPC decoders," in *Int. Symp. Turbo Codes Iter. Inf. Proc.*, Brest, France, Sep. 2010, pp. 201–205.

[6] L. Barnault and D. Declercq, "Fast decoding algorithm for LDPC over GF(2^q)," in *Inf. Theory Worksh.*, Paris, France, Mar. 2003, pp. 70–73.

[7] F. Lazaro, A. Graell i Amat, G. Liva, and B. Matuz, "Symbol message passing decoding of nonbinary low-density parity-check codes," in *Global Commun. Conf.*, Waikoloa, HI, USA, Dec. 2019, pp. 1–5.

[8] A. Ashikhmin, G. Kramer, and S. ten Brink, "Extrinsic information transfer functions: Model and erasure channel properties," *IEEE Trans. Inf. Theory*, vol. 50, no. 11, pp. 2657–2673, 2004.

[9] G. Lechner, T. Pedersen, and G. Kramer, "Analysis and Design of Binary Message Passing Decoders," *IEEE Trans. Commun.*, vol. 60, no. 3, pp. 601–607, Mar. 2012.

[10] G. Liva, B. Matuz, E. Paolini, and M. F. Flanagan, "Non-binary LDPC codes for orthogonal modulations: Analysis and code design," in *IEEE Int. Conf. Commun.*, 2017, pp. 1–6.

[11] *TM Synchronization and Channel Coding*, Blue Book, Issue 2, Consultative Committee for Space Data Systems (CCSDS) Recommendation for Space Data System Standard 131.0.B.2, Aug. 2011.

[12] C. Jones, E. Valles, M. Smith, and J. Villasenor, "Approximate-min constraint node updating for LDPC code decoding," in *Mil. Commun. Conf.*, vol. 1, Boston, MA, USA, May 2003, pp. 157–162.

[13] B. P. Smith, A. Farhood, A. Hunt, F. R. Kschischang, and J. Lodge, "Staircase Codes: FEC for 100 Gb/s OTN," *J. Lightw. Technol.*, vol. 30, no. 1, pp. 110–117, Jan. 2012.