# Error-Correction Performance of Regular Ring-Linear LDPC Codes over Lee Channels

Jessica Bariffi, *Student Member, IEEE*, Hannes Bartz, *Member, IEEE*, Gianluigi Liva, *Senior Member, IEEE* and Joachim Rosenthal, *Fellow, IEEE*

***Abstract*—Most low-density parity-check (LDPC) code constructions are considered over finite fields. In this work, we focus on regular LDPC codes over integer residue rings and analyze their performance with respect to the Lee metric. Their error-correction performance is studied over two channel models, in the Lee metric. The first channel model is a discrete memoryless channel, whereas in the second channel model an error vector is drawn uniformly at random from all vectors of a fixed Lee weight. It is known that the two channel laws coincide in the asymptotic regime, meaning that their marginal distributions match. For both channel models, we derive upper bounds on the block error probability in terms of a random coding union bound as well as sphere packing bounds that make use of the marginal distribution of the considered channels. We estimate the decoding error probability of regular LDPC code ensembles over the channels using the marginal distribution and determining the expected Lee weight distribution of a random LDPC code over a finite integer ring. By means of density evolution and finite-length simulations, we estimate the error-correction performance of selected LDPC code ensembles under belief propagation decoding and a low-complexity symbol message passing decoding algorithm and compare the performances. The analysis developed in this paper may serve to design regular low-density parity-check (LDPC) codes over integer residue rings for storage and cryptographic application.**

***Index Terms*—Belief propagation, Lee metric, LDPC codes, ring-linear codes, symbol message passing decoding, weight enumerator**

## I. Introduction

THE Lee metric has been introduced in [1], [2] for phase shift keying modulation purposes, where the first notion of a channel "matching" the Lee metric appeared. The construction of Lee-metric codes was explored in various contexts ([3], [4], [5], [6], [7]). Currently, the Lee metric is considered for applications in post-quantum cryptography ([8], [9], [10], [11], [12]). It has been shown that the syndrome decoding problem in the Lee metric (originally introduced over $\mathbb{Z}/4\mathbb{Z}$ in [10]) is NP-hard over any integer residue ring modulo $p^s$, where $p$ is a prime [12]. The paper also provides several generic decoding algorithms to attack the syndrome decoding problem. In [12] the authors showed that the Lee metric information set decoding variants are more costly than their counterparts in the Hamming metric. Therefore, the Lee metric is a promising metric to reduce the key sizes or signature sizes. Furthermore, codes in the Lee metric have potential applications in the context of magnetic [13] and DNA [14] storage systems.

In [8] a channel model has been introduced over a $q$-ary ring, that adds to the channel input an error vector of given constant Lee weight. We will refer to this channel as the *constant Lee weight channel*. In the limit of large block length, the single-letter (i.e., marginal) distribution of the error vector elements follows a Boltzmann-like distribution. This distribution results to be the dominant empirical distribution for vectors of a fixed Lee weight, i.e., under the fixed weight constraints, it is the entropy-maximizing distribution. Introducing an error vector of fixed weight is motivated by code-based cryptosystems, where the error vector is typically generated at the encryption side, with a constant Lee weight. The underlying syndrome decoding problem's hardness is highly dependent on the weight of the error term. As the block length of the code grows large, it is not possible to reduce the Lee weight by a scalar multiplication as shown in [8]. The decoding and error-correction performance is additionally determined by the minimum distance of a code. Hence, deriving bounds for the minimum distance is an important task. For the Lee metric several analogue bounds to the Hamming metric, such as the Singleton bound, Gilbert-Varshamov bound, the sphere packing bound, have been developed (see [15], [16], [17]). These bounds are all with respect to the minimum Lee distance.

In this paper, we consider two channel models: The constant Lee weight channel, and a discrete memoryless channel (DMC) matched to the Lee metric [4]. The first is a channel where a constant-weight error pattern is added to the transmitted codeword, where the error pattern is chosen uniformly at random from the set of vectors with fixed Lee weight and length equal to the block length. It is possible to show that, in the limit of large block length, and with Lee weights that are proportional to the block length, the marginal distribution of the additive error term follows the well-known Boltzmann distribution. The second channel is an additive DMC, where

This paper was presented in part at 2022 IEEE Global Communications Conference.

J. Bariffi was with the German Aerospace Center, Münchener Strasse 20, D-82234 Wessling, Germany, and is currently with the Technical University of Munich, Theresienstrasse 90, D-80333 München, Germany (e-mail: jessica.bariffi@tum.de).

H. Bartz and G. Liva are with the German Aerospace Center, Münchener Strasse 20, D-82234 Wessling, Germany (e-mail: {hannes.bartz,gianluigi.liva}@dlr.de).

J. Rosenthal is with the University of Zurich, Institut für Mathematik, Winterthurerstrasse 190, CH-8057 Zürich, Switzerland (e-mail: rosenthal@math.uzh.ch).

J. Rosenthal has been supported in part by the Swiss National Science Foundation under the grant No. 212865. J. Bariffi, H. Bartz and G. Liva acknowledge the financial support by the Federal Ministry of Education and Research of Germany in the program of "Souverän. Digital. Vernetzt." Joint project 6G-RIC, project identification number: 16KISK022.

the additive error term follows the Boltzmann distribution (however, differently from the constant-weight channel, the Lee weight of the error vector is not fixed). We refer to the second channel as *memoryless Lee channel.*

Making use of the marginal distribution of the channels, we derive upper bounds on the error-correction capability achievable by a code for given block length and rate. We derive random coding union bounds for both channels as well as a sphere-packing bound over the memoryless Lee channel, providing a finite-length performance benchmark to evaluate the block error probability of practical coding schemes. In the case of the memoryless Lee channel, we also derive an upper bound on the decoding failure probability of a general linear block code under maximum likelihood (ML) decoding based on the Lee weight distribution (i.e., the Lee distance spectrum) of the code. We compute the average Lee weight distribution of LDPC code ensembles [18] over finite integer rings [19] and analyze its spectral growth rate.

Finally, we study the decoding performance of LDPC codes over finite integer rings over both channel models. We consider LDPC codes over $q$-ary integer residue rings and analyze their performance with respect to the Lee metric from a code ensemble point of view, via density evolution analysis. For simplicity, we focus on regular LDPC code ensembles, since this class of LDPC code ensembles is mainly used in cryptography. The extension to irregular or protograph-based LDPC code ensembles is straightforward — the main difference in the analysis being the introduction of variable/check node degree-dependent generating functions in the Lee distance spectrum analysis, as well as degree-dependent density evolution recursions. The decoding algorithms considered are the well-known belief propagation (BP) decoding algorithm [20], [19] and the symbol message-passing (SMP) algorithm [21]. The SMP decoder was originally defined for the $q$-ary symmetric channel. In this work we adapt the decoder to Lee channels accordingly. The performance of both decoders will additionally be compared to the Lee symbol flipping (LSF) decoder presented in [22]. We provide finite-length simulation results for both the memoryless Lee channel and the constant Lee weight channel for the decoders mentioned. The results are compared to the finite-length performance bounds derived for the corresponding channel model.

The paper is organized as follows. Section II serves as preliminary section, where we state important definitions and results needed throughout the paper. In Section III, we derive finite-length bounds on the block error probability achievable by block codes over Lee channel models. In Section IV, by means of asymptotic enumeration techniques, we derive the average Lee weight spectrum of a regular LDPC code ensembles. The Lee weight spectrum serves then to derive bounds on the error probability in Section V. We then analyze and compare the performance of LDPC codes over both channel models under BP and SMP decoding. We discuss the main ingredients to adapt the SMP from the original setting to the two channel models in the Lee metric, which relies on an assumption for the extrinsic channel probability. We justify this assumption using empirical results. Finally, conclusions follow in Section VI.

## II. Preliminaries

In this section we introduce the basic notation and results required in the course of the paper. In the following we denote by $\mathbb{Z}/q\mathbb{Z}$ the ring of integers modulo $q$, where $q$ is a positive integer. For simplicity, we assume that $\mathbb{Z}/q\mathbb{Z}$ is represented by the set $\{0, 1, \ldots, q-1\}$. The set of units of $\mathbb{Z}/q\mathbb{Z}$ will be denoted by $(\mathbb{Z}/q\mathbb{Z})^{\times}$. By abuse of notation we will call an element of $(\mathbb{Z}/q\mathbb{Z})^n$ a vector of length $n$ and we will denote it by bold lower case letters. Similarly, matrices are denoted by bold upper case letters. For any real number $x$, we use the notation $[x]^+ := \max(0, x)$. We denote by $X$ a random variable over a discrete alphabet $\mathcal{X}$ and let $x \in \mathcal{X}$ be its realization. For every $x \in \mathcal{X}$, we will denote the probability distribution of $X$ by

$$P_X(x) := \mathbb{P}(X = x).$$

Given a positive integer $n$ and an $s$-tuple of nonnegative integers $\mathbf{k} := (k_1, \ldots, k_s)$ satisfying $\sum_{i=1}^{s} k_i = n$, we denote the multinomial coefficient by

$$\binom{n}{\mathbf{k}} := \binom{n}{k_1, \ldots, k_s} = \frac{n!}{k_1! \ldots k_s!}.$$

### A. The Lee Metric

**Definition II.1.** Let $a \in \mathbb{Z}/q\mathbb{Z}$. Its *Lee weight* is defined as

$$\mathrm{wt}_{\mathsf{L}}(a) := \min(a, q-a).$$

For a vector $\mathbf{a} = (a_1, \ldots, a_n) \in (\mathbb{Z}/q\mathbb{Z})^n$ of length $n$, its Lee weight is defined to be the sum of the Lee weights of its entries, i.e.

$$\mathrm{wt}_{\mathsf{L}}(\mathbf{a}) = \sum_{i=1}^{n} \mathrm{wt}_{\mathsf{L}}(a_i).$$

Intuitively, we can view the elements of $\mathbb{Z}/q\mathbb{Z}$ on a circle with equal distances between them. Then the Lee weight of $a \in \mathbb{Z}/q\mathbb{Z}$ is the minimal number of arcs separating $a$ from the origin 0. This yields the following symmetry property of the Lee weight,

$$\mathrm{wt}_{\mathsf{L}}(a) = \mathrm{wt}_{\mathsf{L}}(q-a). \tag{1}$$

Equation (1) implies that the Lee weight of any element in $\mathbb{Z}/q\mathbb{Z}$ can never exceed $\lfloor q/2 \rfloor$. Furthermore, we observe that the Lee weight of $a \in \mathbb{Z}/q\mathbb{Z}$ is always lower bounded by its Hamming weight, denoted by $\mathrm{wt}_{\mathsf{H}}(a)$, which is equal to 1 if $a$ is nonzero and equal to zero otherwise. Hence, similarly we have $\mathrm{wt}_{\mathsf{L}}(a) \leq \mathrm{wt}_{\mathsf{H}}(a)\lfloor q/2 \rfloor$. Equality between the two weights holds if and only $q \in \{2, 3\}$ for every choice of $a$. Hence, for a vector $\mathbf{a} \in (\mathbb{Z}/q\mathbb{Z})^n$ we have

$$\mathrm{wt}_{\mathsf{H}}(\mathbf{a}) \leq \mathrm{wt}_{\mathsf{L}}(\mathbf{a}) \leq n \cdot \lfloor q/2 \rfloor.$$

Similar to the Hamming weight, the Lee weight induces a distance between two vectors.

**Definition II.2.** Let $\mathbf{a}$ and $\mathbf{b}$ be two vectors in $(\mathbb{Z}/q\mathbb{Z})^n$. The *Lee distance* between $\mathbf{a}$ and $\mathbf{b}$ is the Lee weight of their difference, i.e.

$$\mathrm{d}_{\mathsf{L}}(\mathbf{a}, \mathbf{b}) := \mathrm{wt}_{\mathsf{L}}(\mathbf{a} - \mathbf{b}).$$

It is easy to show that the Lee distance is a metric over the finite ring of integers $\mathbb{Z}/q\mathbb{Z}$.

Lemma II.3 shows the expected Lee weight of a randomly chosen element in $\mathbb{Z}/q\mathbb{Z}$.

**Lemma II.3** ([23]). *Let $A$ be a uniformly distributed random variable over $\mathbb{Z}/q\mathbb{Z}$. The expected Lee weight of $A$ is*

$$\delta_q := \mathbb{E}\left(\mathrm{wt_L}(A)\right) = \begin{cases} \left(q^2-1\right)/4q & \text{if } q \text{ is odd,} \\ q/4 & \text{if } q \text{ is even.} \end{cases}$$

*Proof.* As $A$ is chosen uniformly at random from $\mathbb{Z}/q\mathbb{Z}$, we have $\mathbb{P}(A=i) = \frac{1}{q}$ for every $i \in \mathbb{Z}/q\mathbb{Z}$. Then,

$$\mathbb{E}(\mathrm{wt_L}(A)) = \sum_{i=0}^{q-1} \mathrm{wt_L}(i)\mathbb{P}(A=i) = \frac{1}{q}\sum_{i=0}^{q-1}\mathrm{wt_L}(i),$$

where the summation over the Lee weights can be represented as a sum of integers. In fact, if $q$ is odd, then $\sum_{i=0}^{q-1}\mathrm{wt_L}(i) = 2\sum_{i=1}^{(q-1)/2} i$, whereas for $q$ even we have $\sum_{i=0}^{q-1}\mathrm{wt_L}(i) = q/2 + 2\sum_{i=1}^{q/2-1} i$. Applying the formula for the sum of the first $n$ integers, for $n \in \mathbb{N}$, yields the desired statement. □

Let us define now the $n$-dimensional Lee sphere, $S_{t,q}^{(n)}$, (respectively the $n$-dimensional Lee ball, $V_{t,q}^{(n)}$) over $\mathbb{Z}/q\mathbb{Z}$ centered at the origin of radius $t$ by

$$S_{t,q}^{(n)} := \{\mathbf{x} \in (\mathbb{Z}/q\mathbb{Z})^n \mid \mathrm{wt_L}(\mathbf{x}) = t\}$$
$$V_{t,q}^{(n)} := \{\mathbf{x} \in (\mathbb{Z}/q\mathbb{Z})^n \mid \mathrm{wt_L}(\mathbf{x}) \leq t\}.$$

**Lemma II.4.** *[8, Lemma 1] Assume that $\mathbf{x} \in (\mathbb{Z}/q\mathbb{Z})^n$ has been drawn uniformly at random among all vectors of Lee weight $t$. Let $X$ denote the random variable defining the realizations of an entry $x$ of $\mathbf{x}$. As $n$ grows large, for every $i \in \mathbb{Z}/q\mathbb{Z}$, the probability of $X$ taking the value $i$ is given by*

$$\mathbb{P}(X=i) = \frac{1}{Z(\beta)}\exp\left(-\beta\,\mathrm{wt_L}(i)\right) \tag{2}$$

*where $\beta$ is the unique real solution to the weight constraint $t/n = \sum_{i=0}^{q-1}\mathrm{wt_L}(i)\mathbb{P}(X=i)$ and $Z(\beta)$ denotes the normalization constant.*

In the following, let $\delta := t/n$ be the normalized Lee weight. Note that if $\delta = \delta_q$, then $X$ is distributed uniformly over $\mathbb{Z}/q\mathbb{Z}$ and hence $\beta = 0$. Moreover, $\beta > 0$ if and only if $\delta < \delta_q$. The distribution in (2) is closely related to the Boltzmann distribution [24], [25]. The Boltzmann distribution gives the probability that a system will be in a certain state depending on that states' energy and temperature. In statistical mechanics the distribution is used for systems of fixed compositions all being in a thermal equilibrium. Additionally, the distribution maximizes the entropy subject to a mean energy state. In our case the Lee weight may be interpreted as the energy value of a state $e \in \mathbb{Z}/q\mathbb{Z}$. Hence, we will refer to the distribution in (2) as *Boltzmann distribution* and we will denote it by $B_\delta$.

Finally, we introduce the normalized logarithmic surface (respectively, volume) spectra

$$\sigma_{\delta n}^{(n)} := \frac{1}{n}\log_2\left(\left|S_{\delta n,q}^{(n)}\right|\right) \quad \text{and}$$
$$\nu_{\delta n}^{(n)} := \frac{1}{n}\log_2\left(\left|V_{\delta n,q}^{(n)}\right|\right)$$

while their asymptotic counterparts are denoted by

$$\sigma_\delta := \lim_{n\to\infty}\frac{1}{n}\log_2\left(\left|S_{\delta n,q}^{(n)}\right|\right) \quad \text{and}$$
$$\nu_\delta := \lim_{n\to\infty}\frac{1}{n}\log_2\left(\left|V_{\delta n,q}^{(n)}\right|\right).$$

### *B. Information-Theoretic Definitions*

The entropy of $X$ is then defined to be

$$H(X) := H(P_X) = -\sum_{x\in\mathcal{X}} P_X(x)\log_2 P_X(x),$$

where by convention for $P_X(x) = 0$ we set $P_X(x)\log_2 P_X(x) = 0$. We will make use of the following, well-known result.

**Theorem II.5.** *[24, Theorem 2.5.1] Let $X_1, \dots, X_n$ be a sequence of random variables drawn according to a probability distribution $P(x_1, \dots, x_n)$. Then the entropy of the sequence satisfies*

$$H(X_1,\dots,X_n) = \sum_{i=1}^{n} H(X_i \mid X_{i-1},\dots,X_1)$$
$$\leq \sum_{i=1}^{n} H(X_i)$$

*where equality holds if and only if the $X_i$ are independent.*

Given an empirical distribution $\mathbf{p} := (p_1, p_2, \dots, p_{|\mathcal{X}|})$ we have that that for any positive integer $n$ (see [24, Theorem 11.1.3])

$$\frac{1}{(n+1)^{|\mathcal{X}|}}2^{nH(\mathbf{p})} \leq \binom{n}{n\mathbf{p}} \leq 2^{nH(\mathbf{p})}. \tag{3}$$

Consider two probability distributions $P_X(x)$ and $\widetilde{P}_X(x)$ over a shared alphabet $\mathcal{X}$. Their Kullback-Leibler divergence is denoted as

$$D(P_X \,||\, \widetilde{P}_X) := \sum_{x\in\mathcal{X}} P_X(x)\log_2\left(\frac{P_X(x)}{\widetilde{P}_X(x)}\right).$$

An alternative measure of the similarity of two probability distributions is the total variation distance. We define the distance only for discrete probability distributions, since this paper only deals with this case. We follow the description of [26, Proposition 5.2] and define the total variation distance between two distributions $P_X$ and $\widetilde{P}_X$ over $\mathcal{X}$ as

$$\mathsf{TV}(P_X, \widetilde{P}_X) := \frac{1}{2}\sum_{x\in\mathcal{X}}\left|P_X(x) - \widetilde{P}_X(x)\right|.$$

### C. Low-Density Parity-Check Codes over Finite Integer Rings

We will now introduce linear codes over integer residue rings $\mathbb{Z}/q\mathbb{Z}$ and we will focus in particular on LDPC codes over $\mathbb{Z}/q\mathbb{Z}$. A *ring-linear code* $\mathcal{C} \subset (\mathbb{Z}/q\mathbb{Z})^n$ is a $\mathbb{Z}/q\mathbb{Z}$-submodule of $(\mathbb{Z}/q\mathbb{Z})^n$. Similar to codes over finite fields, codes over rings have a length given by $n$ and a $\mathbb{Z}/q\mathbb{Z}$-dimension given by $k := \log_q(|\mathcal{C}|)$. We then refer to $\mathcal{C}$ as $[n, k]$ linear code over $\mathbb{Z}/q\mathbb{Z}$. A code $\mathcal{C}$ can be represented by the kernel of a parity-check matrix $\mathbf{H} \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$ with $m \geq n - k$, i.e.,

$$\mathcal{C} = \left\{\mathbf{x} \in (\mathbb{Z}/q\mathbb{Z})^n \,|\, \mathbf{H}\mathbf{x}^\top = \mathbf{0}^\top\right\}.$$

We denote by $M := |\mathcal{C}|$ the number of codewords in $\mathcal{C}$. Recall that the code rate of an $[n, k]$ linear code $\mathcal{C}$ of size $M$ over $\mathbb{Z}/q\mathbb{Z}$ is given by

$$R_2 = \frac{\log_2 M}{n} \qquad \text{bits per channel use}$$

or

$$R = \frac{\log_q M}{n} \qquad \text{symbols per channel use.}$$

depending on the choice of logarithm's base.

Different to codes over finite fields, a ring-linear code $\mathcal{C} \subseteq (\mathbb{Z}/q\mathbb{Z})^n$ does not always admit a basis. If it admits a basis, we call $\mathcal{C}$ a *free code*. In that case, a parity-check matrix $\mathbf{H}$ is of size $(n-k) \times n$. LDPC codes [18] are binary linear error-correcting codes characterized by a sparse parity-check matrix. In [19], the authors analyzed LDPC codes over $\mathbb{Z}/q\mathbb{Z}$ defining the nonzero entries of the parity-check matrix over the units $(\mathbb{Z}/q\mathbb{Z})^\times$. Restricting to only unit elements as nonzero entries of a parity-check matrix immediately implies that the code is free. In this way, when randomly drawing the nonzero entries of a parity-check matrix among the unit elements, we assure that the resulting LDPC code is always free. This is not always true when drawing the nonzero entries also among the zero divisors. Additionally, allowing zero divisors in a parity-check matrix can yield to the situation where there is a column whose nonzero entries are all zero divisors. Over $\mathbb{Z}/p^s\mathbb{Z}$, for a prime number $p$, the resulting code would have a minimum Lee distance of at most $\lfloor p^s/2\rfloor$ (see [19] for more details). In the following, let $\mathcal{C}$ always denote an $[n, k]$ linear block code over $\mathbb{Z}/q\mathbb{Z}$ and let $\mathbf{H} \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$ be a parity-check matrix of $\mathcal{C}$, where $m \geq n-k$ and where $m = n-k$ if and only if the code $\mathcal{C}$ is free. A parity-check matrix $\mathbf{H}$ can be described by a bipartite graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ consisting of a set of vertices $\mathcal{V}$ and a set of edges $\mathcal{E}$ connecting the vertices. The set of vertices consists of two disjoint sets: the set of variable nodes (VNs) $\{\mathsf{v}_1, \ldots, \mathsf{v}_n\}$, representing the columns of $\mathbf{H}$, and the set of check nodes (CNs) $\{\mathsf{c}_1, \ldots, \mathsf{c}_m\}$, representing the rows of $\mathbf{H}$. A variable node $\mathsf{v}_j$ is connected to a check node $\mathsf{c}_i$ by an edge if and only if the corresponding entry $h_{ij}$ in the parity-check matrix is nonzero. The edge carries as label the entry $h_{ij}$. The degree $d_\mathsf{v}$ of a variable node $\mathsf{v}$ is the number of edges connected to $\mathsf{v}$. The neighbors $\mathcal{N}(\mathsf{v})$ of a variable node $\mathsf{v}$ is the set of check nodes connected to $\mathsf{v}$. Similarly, we define the degree $d_\mathsf{c}$ and the neighbors $\mathcal{N}(\mathsf{c})$ of a check node $\mathsf{c}$.

We consider regular nonbinary LDPC codes which have a constant variable node degree $d_\mathsf{v} = d_v$ and a constant check node degree $d_\mathsf{c} = d_c$. We denote by $\mathscr{C}^n_{d_v,d_c}$ the unstructured regular LDPC code ensemble of length $n$, i.e. the set of all LDPC codes defined by an $(m \times n)$ parity-check matrix, whose associated bipartite graph has constant variable node degree $d_v$ and constant check node degree $d_c$. This ensemble has then the designed rate $R_0 = 1 - m/n$. As proposed in [19], when sampling an LDPC code from $\mathscr{C}^n_{d_v,d_c}$, we assume that the nonzero entries of a parity-check matrix are drawn independently and uniformly at random from the set of units $(\mathbb{Z}/q\mathbb{Z})^\times$.

### D. Message Passing Decoders

We briefly recall two message passing algorithms for nonbinary LDPC codes. The first algorithm is the well-known (nonbinary) BP algorithm. The second algorithm is a message passing algorithm where the messages exchanged between variable and check nodes are hard symbol estimates. The latter algorithm, dubbed SMP, generalizes the Gallager-B algorithm [18] and binary message-passing (BMP) algorithm [27] to nonbinary alphabets.

Let us fix some notation used in the description of the two decoders. We denote by $\boldsymbol{m}_{\mathsf{v}\to\mathsf{c}}$ the message sent from variable node $\mathsf{v}$ to a neighboring check node $\mathsf{c}$ and vice versa $\boldsymbol{m}_{\mathsf{c}\to\mathsf{v}}$ is the message sent from $\mathsf{c}$ to $\mathsf{v}$. Furthermore, we will denote the likelihood at the variable node $\mathsf{v}$ input (associated with the corresponding channel observation) by

$$\boldsymbol{m}_\mathsf{v} := \left(P_{Y|X}(y \mid 0), \ldots, P_{Y|X}(y \mid q-1)\right),$$

i.e., this is the vector of probabilities of the channel output $y$, conditioned on the $q$ possible channel input values. For every connected variable node $\mathsf{v}$ and check node $\mathsf{c}$ we denote by $h_{\mathsf{cv}}$ the corresponding entry in the parity-check matrix $\mathbf{H}$. Note, since the nonzero entries of $\mathbf{H}$ were chosen to be units modulo $q$, the inverse $h_{\mathsf{cv}}^{-1}$ is guaranteed to exist.

#### 1) Belief Propagation Decoding:

We consider now the BP algorithm for nonbinary LDPC codes over finite rings. The decoder consists of four main steps that are outlined below, where Step 2 and 3 are repeated at most $\ell_{\max}$ times. For every connected variable node $\mathsf{v}$ and check node $\mathsf{c}$ we let $\mathbf{\Pi}_{\mathsf{cv}}$ be the $(q \times q)$ permutation matrix induced by $h_{\mathsf{cv}}$.[1]

1) **Initialization.** Each variable node $\mathsf{v}$ receives the channel observation in the form of $\boldsymbol{m}_\mathsf{v}$. Then, the variable node $\mathsf{v}$ sends to each $\mathsf{c} \in \mathcal{N}(\mathsf{v})$ the permuted channel observation, i.e.,

$$\boldsymbol{m}_{\mathsf{v}\to\mathsf{c}} = \boldsymbol{m}_\mathsf{v} \cdot \mathbf{\Pi}_{\mathsf{cv}}.$$

2) **CN-to-VN step.** Consider a given check node $\mathsf{c}$ and a neighboring variable node $\mathsf{v} \in \mathcal{N}(\mathsf{c})$. For the message

[1] In fact, consider two random elements $X, X' \in \mathbb{Z}/q\mathbb{Z}$ with probability distributions $P(X)$ and $Q(X')$, respectively. Denote by $\boldsymbol{m} = (P(0), P(1), \ldots, P(q-1))$ and by $\boldsymbol{m}' = (Q(0), Q(1), \ldots, Q(q-1))$. If $X' = hX$ for $h \in (\mathbb{Z}/q\mathbb{Z})^\times$, then since $Q(X') = P(hX)$ the distribution $\boldsymbol{m}'$ is obtained by permuting $\boldsymbol{m}$ with a permutation that is completely determined by the multiplication coefficient $h$.

$\boldsymbol{m}_{\mathsf{c}\to\mathsf{v}}$, the check node computes the circular convolution A of the incoming messages $\boldsymbol{m}_{\mathsf{v}'\to\mathsf{c}}$ from all neighboring variable nodes $\mathsf{v}' \in \mathcal{N}(\mathsf{c}) \setminus \{\mathsf{v}\}$ as

$$\mathbf{u} = \mathop{\circledast}_{\mathsf{v}'\in\mathcal{N}(\mathsf{c})\setminus\{\mathsf{v}\}} \boldsymbol{m}_{\mathsf{v}'\to\mathsf{c}}$$

and sends to every neighboring variable node $\mathsf{v} \in \mathcal{N}(\mathsf{c})$ a permuted version of $\mathbf{u}$ according to the permutation $\boldsymbol{\Pi}_{\mathsf{cv}}^{-1}$, i.e., the CN-to-VN message is

$$\boldsymbol{m}_{\mathsf{c}\to\mathsf{v}} = \mathbf{u} \cdot \boldsymbol{\Pi}_{\mathsf{cv}}^{-1}.$$

3) **VN-to-CN step.** The variable node $\mathsf{v}$ computes the Schur product $\odot$ of all incoming messages but the one from check node $\mathsf{c}$ and normalizes the result by a constant $K$ (to obtain a proper probability vector)

$$\mathbf{v} = K \bigodot_{\mathsf{c}'\in\mathcal{N}(\mathsf{v})\setminus\{\mathsf{c}\}} \boldsymbol{m}_{\mathsf{c}'\to\mathsf{v}}.$$

Finally, it applies the permutation matrix $\boldsymbol{\Pi}_{\mathsf{cv}}$ to the vector $\mathbf{v}$ and sends the following message to the check node $\mathsf{c}$

$$\boldsymbol{m}_{\mathsf{v}\to\mathsf{c}} = \mathbf{v} \cdot \boldsymbol{\Pi}_{\mathsf{cv}}.$$

4) **Final decision.** The final decision happens at the variable node side. After at most $\ell_{\max}$ iterations of steps 2 and 3 each variable node computes the Schur product of all incoming messages, yielding the a posteriori probability (APP) estimate

$$\boldsymbol{m}_{\mathsf{v}}^{\mathsf{APP}} = \bigodot_{\mathsf{c}\in\mathcal{N}(\mathsf{v})} \boldsymbol{m}_{\mathsf{c}\to\mathsf{v}}.$$

The decision $\hat{x}$ is the index of the maximal entry of $\boldsymbol{m}_{\mathsf{v}}^{\mathsf{APP}}$

$$\hat{x} = \arg\max_{i\in\mathbb{Z}/q\mathbb{Z}} m_{\mathsf{v},i}^{\mathsf{APP}}.$$

### 2) Symbol Message Passing Decoding:

The SMP algorithm is a message-passing algorithm for non-binary LDPC codes, where each message exchanged by a variable node/check node pair is a symbol, i.e., a hard estimate of the codeword symbol associated with the variable node. Following the principle outlined in [27], the messages sent by check nodes to variable nodes are modeled as observations at the output a $q$-ary input, $q$-ary output DMC. By doing so, the messages at the input of each variable node can be combined by multiplying the respective likelihoods (or by summing the respective log-likelihoods), providing a simple update rule at the variable nodes.

Assume we have a DMC over $\mathbb{Z}/q\mathbb{Z}$ with output $w$ and channel law $P_{W\,|\,X}(w\,|\,x)$. We define the log-likelihood of $w$ given $x$ by $L_x(w) := \log\big(P_{W\,|\,X}(w\,|\,x)\big)$ and the log-likelihood vector by

$$\mathbf{L}(w) := (L_0(w), L_1(w), \ldots, L_{q-1}(w)).$$

With a slight abuse of notation, we will use the $\mathbf{L}(\cdot)$ for different channels, where the channel law to be applied is made clear by the argument.

1) **Initialization.** The decoder is initialized by forwarding the channel observation $y$ to every variable node $\mathsf{v}$. Then, the variable node $\mathsf{v}$ sends to each $\mathsf{c} \in \mathcal{N}(\mathsf{v})$

$$m_{\mathsf{v}\to\mathsf{c}} = y.$$

2) **CN-to-VN step.** Consider a given check node $\mathsf{c}$ and a neighboring variable node $\mathsf{v} \in \mathcal{N}(\mathsf{c})$. For the message $\boldsymbol{m}_{\mathsf{c}\to\mathsf{v}}$, the check node computes

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

3) **VN-to-CN step.** At each variable node $\mathsf{v}$, incoming messages are treated as observations of the codeword symbol at the output of an "extrinsic channel" ([27], [28]) modelled as a $q$-ary symmetric channel ($q$-SC) with error probability $\xi \in [0,1]$, i.e., with conditional probability

$$P_{M\,|\,X}(m\,|\,x) = \begin{cases} 1-\xi & \text{if } m = x \\ \xi/(q-1) & \text{otherwise} \end{cases}. \tag{4}$$

For the calculation of the message to be sent of each check node $\mathsf{c} \in \mathcal{N}(\mathsf{v})$, (4) is used to compute the log-likelihood vector

$$\mathbf{E} = \mathbf{L}(y) + \sum_{\mathsf{c}'\in\mathcal{N}(\mathsf{v})\setminus\{\mathsf{c}\}} \mathbf{L}\left(m_{\mathsf{c}'\to\mathsf{v}}\right). \tag{5}$$

For each $\mathsf{c} \in \mathcal{N}(\mathsf{v})$, the message sent by the variable node $\mathsf{v}$ is then

$$m_{\mathsf{v}\to\mathsf{c}} = \arg\max_{i\in\mathbb{Z}/q\mathbb{Z}} E_i.$$

4) **Final decision.** After at most $\ell_{\max}$ iterations for each variable node $\mathsf{v}$ we compute

$$\mathbf{L}^{\mathsf{FIN}} = \mathbf{L}(y) + \sum_{\mathsf{c}\in\mathcal{N}(\mathsf{v})} \mathbf{L}\left(m_{\mathsf{c}\to\mathsf{v}}\right).$$

Then the final decision, $\hat{x}$, is the index of the maximal entry of $\mathbf{L}^{\mathsf{FIN}}$, i.e.,

$$\hat{x} = \arg\max_{i\in\mathbb{Z}/q\mathbb{Z}} L_i^{\mathsf{FIN}}.$$

Note that the extrinsic channel of (4) is modelled as a $q$-SC with error probability $\xi$. As it will be shown in Section V-B, this choice yields an accurate description of the extrinsic channel conditional probability, despite of its simplicity. The extrinsic channel parameter $\xi$ is iteration-dependent. Its evaluation can be performed via Monte Carlo simulations, or by using estimates that follow from density evolution (DE) analysis [27], [21].

## E. Lee Channels

We consider classical additive channel models over the $q$-ary alphabet $\mathbb{Z}/q\mathbb{Z}$. In the constant Lee weight channel, a random error vector $\mathbf{e} \in (\mathbb{Z}/q\mathbb{Z})^n$ of fixed Lee weight $\mathrm{wt}_{\mathsf{L}}(\mathbf{e}) = t$ is added to the channel input $\mathbf{x} \in \mathcal{C}$, i.e., the channel output is

$$\mathbf{y} = \mathbf{x} + \mathbf{e}.$$

More specifically, the error vector $\mathbf{e}$ is drawn uniformly at random over the Lee sphere $S_{t,q}^{(n)}$ of radius $t = \delta n$. Hence, the channel transition probability for the constant Lee weight channel is

$$P_{\mathbf{Y}\,|\,\mathbf{X}}(\mathbf{y}\,|\,\mathbf{x}) = \begin{cases} \left|S_{\delta n,q}^{(n)}\right|^{-1} & \text{if } \mathrm{d}_{\mathsf{L}}(\mathbf{y},\mathbf{x}) = \delta n, \\ 0 & \text{otherwise.} \end{cases}$$

As a consequence of Lemma II.4, the marginal distribution of the error terms follows, for large $n$, the Boltzmann distribution

$$P_E(e) = \frac{1}{Z(\beta)} \exp\left(-\beta\,\mathrm{wt}_{\mathsf{L}}(e)\right) \tag{6}$$

where $\beta$ follows by enforcing $\mathbb{E}\left(\mathrm{wt}_{\mathsf{L}}(E)\right) = \delta$. In the course of this paper we will denote the Boltzmann distribution from Equation (6) by $B_\delta$.

The memoryless Lee channel is a DMC defined by

$$y = x + e$$

where $y, x, e \in \mathbb{Z}/q\mathbb{Z}$, and where the probability distribution of $e$ matches the marginal distribution of the constant Lee weight channel of (6). We denote the expected normalized Lee weight of $\mathbf{e} \in \mathbb{Z}/q\mathbb{Z}$ by

$$\delta = \mathbb{E}\left(\frac{1}{n}\,\mathrm{wt}_{\mathsf{L}}(\mathbf{E})\right).$$

As the channel is memoryless, we have again $\delta = \mathbb{E}\left(\mathrm{wt}_{\mathsf{L}}(E)\right)$.

## III. Finite-Length Bounds for Lee Channels

In this section we are going to derive bounds on the error probability achievable by an $[n,k]$ code over both the constant Lee weight channel and the memoryless Lee channel defined in Section II-E.[2]. In the first case we will see an achievability bound in terms of a random coding union bound. For the memoryless Lee channel we will derive an upper bound again in terms of a random coding union (RCU) bound as well as a converse bound, meaning a lower bound, achievable by any $[n,k]$ code in terms of a sphere-packing bound.

For both channel models we distinguish between ML decoding and minimum distance (MD) decoding, that is, given a received word $y \in \mathbb{Z}/q\mathbb{Z}$, we consider the ML decoding rule

$$\hat{\mathbf{x}}_{\mathrm{ML}} = \operatorname*{argmax}_{\mathbf{x}\in\mathcal{C}} P_{\mathbf{Y}\,|\,\mathbf{X}}(\mathbf{y}\,|\,\mathbf{x})$$

and the MD decoding rule

$$\hat{\mathbf{x}}_{\mathrm{MD}} = \operatorname*{argmin}_{\mathbf{x}\in\mathcal{C}} \mathrm{d}_{\mathsf{L}}(\mathbf{y},\mathbf{x}).$$

Note that the two decoding rules coincide over the memoryless Lee channel for $\delta \leq \delta_q$. In the constant Lee weight channel, the ML decoder gives a list of all codewords which are at distance $\delta n$ from the received word $\mathbf{y}$ and it outputs one of the codewords in this list randomly. Hence, the two decoding rules for the constant Lee weight channel coincide whenever $\delta n$ is within the decoding radius of the code $\mathcal{C}$.

### A. Bounds on the Lee Spheres and Lee Balls

Before proceeding with the derivation of the error probability bounds, we first derive upper bounds on the size of a Lee sphere and a Lee ball, respectively.

We denote by $H_\delta := H(B_\delta)$ the entropy of the Boltzmann distribution with parameter $\delta$ and we introduce the notation

$$H_\delta^+ := \begin{cases} H_\delta & 0 \leq \delta \leq \delta_q \\ \log_2(q) & \delta_q < \delta < r. \end{cases}$$

**Lemma III.1** (Growth rate of the surface spectrum)**.** *For any positive integer $\delta n$ the surface spectrum is upper bounded by*

$$\sigma_{\delta n}^{(n)} \leq H_\delta.$$

*In particular, as $n$ grows large it holds that $\sigma_\delta = H_\delta$.*

*Proof.* Let $\mathbf{X} = (X_1, \dots, X_n)$ be a finite sequence of random variables $X_i$ chosen uniformly at random in the Lee sphere $S_{\delta n,q}^{(n)}$. Since $\mathbf{X}$ is uniformly distributed in the sphere, its entropy is given by $H(\mathbf{X}) = \log_2\left(\left|S_{\delta n,q}^{(n)}\right|\right)$. Hence, the normalized logarithmic surface area is

$$\sigma_{\delta n}^{(n)} = \frac{1}{n} H(\mathbf{X}).$$

The chain rule for the entropy, Theorem II.5, and the fact that the $X_i$´s are identically distributed, yield

$$H(\mathbf{X}) \leq \sum_{i=1}^{n} H(X_i) = nH(X_1).$$

Since the Boltzmann distribution $B_\delta$ is the distribution of $X_1$ maximizing the entropy under the constraint that $\mathbb{E}(\mathrm{wt}_{\mathsf{L}}(X_1)) = \delta$, the desired upper bound follows. To get the asymptotic result it suffices to take limits on both sides of the inequality. □

**Lemma III.2** (Growth rate of the volume spectrum)**.** *For any positive integer $\delta n$ the volume spectrum is upper bounded by*

$$\nu_{\delta n}^{(n)} \leq H_\delta^+.$$

*In particular, as $n$ grows large we have that $\nu_\delta = H_\delta^+$.*

*Proof.* The proof follows in a similar fashion to the proof of the growth rate of the surface spectrum. Consider a random vector $\mathbf{X} = (X_1, \dots, X_n)$ chosen uniformly at random over $V_{\delta n,q}^{(n)}$. Hence, $\mathrm{wt}_{\mathsf{L}}(\mathbf{x}) \leq \delta n$, where $\mathbf{x}$ denotes the realization of $\mathbf{X}$. It holds that

$$\log_2\left(\left|V_{\delta n,q}^{(n)}\right|\right) = H(\mathbf{X}),$$

which implies, using again Theorem II.5, that

$$\nu_{\delta n}^{(n)} = \frac{1}{n} H(\mathbf{X}) \leq H(X_1).$$

Note that $H(X_1) \leq \log_2(q)$ for any parameter of $\delta \in [0, r]$. Hence, again since $B_\delta$ maximizes the entropy under the constraint $\mathbb{E}(\mathrm{wt}_{\mathsf{L}}(X_1)) \leq \delta$, we observe that $H(X_1) \leq H_\delta^+$ which yields the first statement of the lemma. To prove the latter statement it suffices to take the limit as $n$ tends to infinity. □

[2] Several of bounds minimum distance achievable by $[n,k]$ codes can be found in [15], [16], [17]

### B. Error Probability Bounds for the Constant Lee Weight Channel

We consider an $[n,k]$ code $\mathcal{C}$ of cardinality $|\mathcal{C}| = q^k =: M$ over $\mathbb{Z}/q\mathbb{Z}$, and we focus on the constant Lee weight channel where the additive error term is of fixed Lee weight $\delta n$. We denote by $P_B(\mathcal{C})$ the block error probability of the code $\mathcal{C}$ under a given decoding rule.

**Theorem III.3** (Random Coding Union Bound, ML Decoding)**.** *Let $\mathcal{C} \subset (\mathbb{Z}/q\mathbb{Z})^n$ be a random code of rate $R_2$. The average ML decoding error probability of $\mathcal{C}$ used to transmit over a constant Lee weight channel satisfies*

$$\mathbb{E}\left(P_B(\mathcal{C})\right) < 2^{-n\left[\log_2 q - \sigma_{\delta n}^{(n)} - R_2\right]^+}.$$

*Proof.* Consider first the pairwise error probability $\mathsf{PEP}(\mathbf{x},\mathbf{y})$ for fixed $\mathbf{x}$ and $\mathbf{y}$, where $\mathbf{x}$ is the transmitted codeword, $\mathbf{y}$ is the channel output and $\widetilde{\mathbf{X}}$ is a random codeword distributed uniformly over $(\mathbb{Z}/q\mathbb{Z})^n$. By breaking ties always towards $\widetilde{\mathbf{X}}$, we can upper bound the pairwise error probability as

$$\begin{aligned}\mathsf{PEP}(\mathbf{x},\mathbf{y}) &\le \mathbb{P}\left(P_{\mathbf{Y}\,|\,\mathbf{X}}(\mathbf{y}\,|\,\mathbf{x}) = P_{\mathbf{Y}\,|\,\mathbf{X}}(\mathbf{y}\,|\,\widetilde{\mathbf{X}})\right)\\ &= \mathbb{P}\left(\mathrm{d}_{\mathsf{L}}(\mathbf{y},\widetilde{\mathbf{X}}) = \delta n\right)\\ &= \frac{\left|S_{\delta n,q}^{(n)}\right|}{q^n}.\end{aligned}$$

The union bound on the block error probability is obtained by multiplying the result by $M-1$. By observing that the pairwise error probability does not depend on $\mathbf{x},\mathbf{y}$, we get

$$\begin{aligned}\mathbb{E}\left(P_B(\mathcal{C})\right) &\le \min\left(1, (M-1)\mathsf{PEP}(\mathbf{x},\mathbf{y})\right)\\ &< \min\left(1,\, M\frac{\left|S_{\delta n,q}^{(n)}\right|}{q^n}\right)\\ &= 2^{-n\left[\log_2 q - \sigma_{\delta n}^{(n)} - R_2\right]^+}.\end{aligned}$$

□

Owing to Lemma III.1, the bound can be loosened yielding the simple form described in the following corollary.

**Corollary III.4.** *The average ML decoding error probability of a random code $\mathcal{C} \subset (\mathbb{Z}/q\mathbb{Z})^n$ of rate $R_2$ used to transmit over a constant Lee weight channel satisfies*

$$\begin{aligned}\mathbb{E}(P_B(\mathcal{C})) &< 2^{-n[\log_2 q - H_\delta - R_2]^+}\\ &= 2^{-n[D(B_q\,||\,\mathcal{U}(\mathbb{Z}/q\mathbb{Z})) - R_2]^+}.\end{aligned}$$

In terms of MD decoding, the two results can be proven in a similar fashion, considering all codewords of distance up to $\delta n$, i.e., instead of working over the sphere $S_{\delta n,q}^{(n)}$ only we extend to the ball $V_{\delta n,q}^{(n)}$. Then the MD counterparts of Theorem III.3 and its consequence, Corollary III.4, are given in the following two results.

**Theorem III.5** (Random Coding Union Bound, MD decoding)**.** *Let $\mathcal{C} \subset (\mathbb{Z}/q\mathbb{Z})^n$ be a random code of rate $R_2$. The average MD decoding error probability of $\mathcal{C}$ used to transmit over a constant Lee weight channel satisfies*

$$\mathbb{E}(P_B(\mathcal{C})) < 2^{-n\left[\log_2 q - \nu_{\delta n}^{(n)} - R_2\right]^+}.$$

*Proof.* Consider first the pairwise error probability under the assumption that $\mathbf{x}$ is the transmitted codeword, $\mathbf{y}$ is the channel output and $\widetilde{\mathbf{X}}$ is a random codeword distributed uniformly over $(\mathbb{Z}/q\mathbb{Z})^n$. By breaking ties always towards $\widetilde{\mathbf{X}}$, we have

$$\begin{aligned}\mathsf{PEP}(\mathbf{x},\mathbf{y}) &\le \mathbb{P}\left(\mathrm{d}_{\mathsf{L}}(\mathbf{y},\mathbf{x}) \ge \mathrm{d}_{\mathsf{L}}(\mathbf{y},\widetilde{\mathbf{X}})\right)\\ &= \mathbb{P}(\mathrm{d}_{\mathsf{L}}(\mathbf{y},\widetilde{\mathbf{X}}) \le \delta n)\\ &= \frac{\left|V_{\delta n}^{(n)}\right|}{q^n}.\end{aligned}$$

The union bound on the block error probability can be obtained by multiplying the result by $M-1$. By observing that the pairwise error probability does not depend on $\mathbf{x},\mathbf{y}$, we get

$$\begin{aligned}\mathbb{E}(P_B(\mathcal{C})) &\le \min\left(1, (M-1)\mathsf{PEP}(\mathbf{x},\mathbf{y})\right)\\ &< \min\left(1, M\frac{\left|V_{\delta n}^{(n)}\right|}{q^n}\right)\\ &= 2^{-n\left[\log_2 q - \nu_{\delta n}^{(n)} - R_2\right]^+}.\end{aligned}$$

□

Owing to Lemma III.2, the bound can be loosened yielding the simple form described in Corollary III.6.

**Corollary III.6.** *The average MD decoding error probability of a random code $\mathcal{C} \subset (\mathbb{Z}/q\mathbb{Z})^n$ of rate $R_2$ used to transmit over a constant Lee weight channel satisfies*

$$\mathbb{E}(P_B(\mathcal{C})) < 2^{-n\left[\log_2 q - H_\delta^+ - R_2\right]^+}.$$

Figure 1 depicts the upper bounds based on Theorem III.5 and Corollary III.6 for MD decoding, for $[500, 250]$ codes over $\mathbb{Z}/7\mathbb{Z}$. The bound of Corollary III.6 is only slightly looser than the one provided by Theorem III.5. A similar result holds for the bounds of Theorem III.3 and Corollary III.4, under ML decoding.

### C. Error Probability Bounds for the Memoryless Lee Channel

We consider next a memoryless Lee channel with expected normalized Lee weight of the error pattern $\delta$. We restrict the attention to the case $\delta \le \delta_q$. Recall that, in this regime, the ML and the MD decoding rules coincide since the ML decoder gives a list of all codewords which are at distance $\delta n$ from the received word $\mathbf{y}$ and it outputs one of the codewords in this list randomly.

**Theorem III.7** (Random Coding Union Bound)**.** *Let $\mathcal{C} \subset (\mathbb{Z}/q\mathbb{Z})^n$ be a random code of rate $R_2$. The average ML/MD decoding error probability of $\mathcal{C}$ used to transmit over a memoryless Lee channel with expected normalized Lee weight $\delta$ of the error pattern satisfies*

$$\mathbb{E}\left(P_B(\mathcal{C})\right) < \mathbb{E}\left(2^{-n\left[\log_2 q - \nu_L^{(n)} - R_2\right]^+}\right)$$

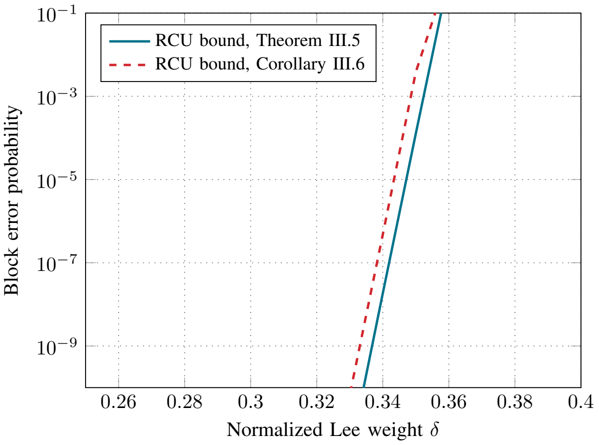

Fig. 1. Random coding union bounds under MD decoding based on Theorem III.5 and Corollary III.6 for the parameters $n = 500$ and $k = 250$ over $\mathbb{Z}/7\mathbb{Z}$.

*where the expectation is taken over the distribution of the Lee weight* $L = \mathrm{wt}_\mathsf{L}(\mathbf{E})$.

*Proof.* Let $\mathbf{E} \in (\mathbb{Z}/q\mathbb{Z})^n$ with $\mathrm{wt}_\mathsf{L}(\mathbf{E}) = L$, $\widetilde{\mathbf{X}}$ is a random codeword distributed uniformly over $(\mathbb{Z}/q\mathbb{Z})^n$, $\mathbf{x}$ the transmitted codeword and $\mathbf{y}$ the channel output. We estimate the pairwise error probability of $\mathbf{x}$ and $\mathbf{y}$ given that $\mathrm{wt}_\mathsf{L}(\mathbf{E}) = L$. That is, by breaking ties always towards $\widetilde{\mathbf{X}}$, we get

$$\begin{aligned}\mathsf{PEP}_L(\mathbf{x},\mathbf{y}) &\leq \mathbb{P}\Big(\mathrm{d}_\mathsf{L}(\mathbf{y},\mathbf{x}) \geq \mathrm{d}_\mathsf{L}(\mathbf{y},\widetilde{\mathbf{X}}) \,|\, \mathrm{wt}_\mathsf{L}(\mathbf{E}) = L\Big)\\ &= \mathbb{P}\left(\mathrm{d}_\mathsf{L}(\mathbf{y},\widetilde{\mathbf{X}}) \leq L \,|\, \mathrm{wt}_\mathsf{L}(\mathbf{E}) = L\right)\\ &= \frac{\left|V_L^{(n)}\right|}{q^n}.\end{aligned}$$

The union bound on the block error probability can be obtained by multiplying the result by $M - 1$. By observing that the pairwise error probability does not depend on $\mathbf{x}, \mathbf{y}$, we get

$$\begin{aligned}\mathbb{E}(P_B(\mathcal{C}) \,|\, \mathrm{wt}_\mathsf{L}(\mathbf{E}) = L) &\leq \min(1, (M-1)\mathsf{PEP}_L(\mathbf{x},\mathbf{y}))\\ &< \min\left(1, M\frac{\left|V_L^{(n)}\right|}{q^n}\right)\\ &= 2^{-n\left[\log_2 q - \nu_L^{(n)} - R_2\right]^+}.\end{aligned}$$

Then, taking the expectation with respect to the Lee weight of $\mathbf{E}$ yields the desired result. □

A direct consequence using Lemma III.2 is captured in Corollary III.8. Its proof follows similar to the constant Lee weight case.

**Corollary III.8.** *The average ML/MD decoding error probability of a random code* $\mathcal{C} \subset (\mathbb{Z}/q\mathbb{Z})^n$ *of rate* $R_2$ *used to transmit over a memoryless Lee channel satisfies*

$$\mathbb{E}(P_B(\mathcal{C})) < \mathbb{E}\left(2^{-n\left[\log_2 q - H^+_{L/n} - R_2\right]^+}\right)$$

*where the expectation is taken over the distribution of the Lee weight* $L = \mathrm{wt}_\mathsf{L}(\mathbf{E})$.

Following the idea of [29, Section 5.8], we provide next a lower bound on the block error probability achievable by *any* $[n, k]$ code over the memoryless Lee channel.

**Theorem III.9** (Sphere-Packing Bound)**.** *The block error probability of any code* $\mathcal{C} \subseteq (\mathbb{Z}/q\mathbb{Z})^n$ *of rate* $R_2$ *over a memoryless Lee channel is lower bounded as*

$$\begin{aligned}P_B(\mathcal{C}) >& \frac{1}{Z(\beta)^n} \sum_{d=d_0+1}^{rn} \left|S_{d,q}^{(n)}\right| \exp(-\beta d)\\ &+ \frac{1}{Z(\beta)^n}\left(\left|S_{d_0,q}^{(n)}\right| - \xi\right) \exp(-\beta d_0)\end{aligned}$$

*where* $d_0$ *and* $\xi$ *are chosen so that*

$$\sum_{d=0}^{d_0-1} \left|S_{d,q}^{(n)}\right| + \xi = 2^{n(\log_2(q) - R_2)} \quad \textit{and}$$

$$0 < \xi \leq \left|S_{d_0,q}^{(n)}\right|.$$

*Proof.* The proof follows closely the analogous proof for the binary symmetric channel provided in [29, Section 5.8]. Let $\mathcal{C} \subseteq (\mathbb{Z}/q\mathbb{Z})^n$ be a code of rate $R_2 = \frac{\log_2(M)}{n}$ and let $\mathbf{x}_1, \dots, \mathbf{x}_M$ denote its codewords. Furthermore, we define for each codeword $\mathbf{x}_i$, the set $\mathcal{Y}_i$ of output sequences $\mathbf{y}$ such that $\mathbf{y}$ is decoded into $\mathbf{x}_i$. Within a decision region $\mathcal{Y}_i$, we let $A_{d,i}$ denote the number of sequences $\mathbf{y} \in \mathcal{Y}_i$ such that $\mathrm{d}_\mathsf{L}(\mathbf{y}, \mathbf{x}_i) = d$. The overall probability of correct decoding can then be computed as

$$\begin{aligned}P_{\mathsf{correct}} &= \frac{1}{M} \sum_{i=1}^{M} \sum_{\mathbf{y} \in \mathcal{Y}_i} P_{\mathbf{Y}\,|\,\mathbf{X}}(\mathbf{y} \,|\, \mathbf{x}_i)\\ &= \frac{1}{M} \sum_{i=1}^{M} \sum_{d=0}^{n\lfloor q/2 \rfloor} A_{d,i} \frac{1}{Z(\beta)^n} \exp(-\beta d).\end{aligned}$$

This implies that the block error probability $P_B(\mathcal{C})$ is computed as

$$\begin{aligned}P_B(\mathcal{C}) &= 1 - P_{\mathsf{correct}}\\ &= \frac{1}{M} \sum_{i=1}^{M} \sum_{d=0}^{n\lfloor q/2 \rfloor} \left(\left|S_{d,q}^{(n)}\right| - A_{d,i}\right) \frac{1}{Z(\beta)^n} \mathrm{e}^{-\beta d}. \quad (7)\end{aligned}$$

To obtain the desired lower bound, we minimize the expression on the right hand side of (7). The expression is minimized subject to the constraints

- $A_{d,i} \leq \left|S_{d,q}^{(n)}\right|$, for every $d \in \{0, \dots, n\lfloor q/2 \rfloor\}$ and $i = \{1, \dots, M\}$, and
- $\sum_{i=0}^{M} \sum_{d=0}^{n\lfloor q/2 \rfloor} A_{d,i} \leq q^n$.

It can be shown that the minimum is achieved for

$$A_{d,i} = \begin{cases} \left|S_{d,q}^{(n)}\right| & 0 \leq d \leq d_0 - 1 \\ 0 & d_0 + 1 \leq d \leq n\lfloor q/2 \rfloor \end{cases}, \quad (8)$$

where $d_0$ is chosen such that

$$\sum_{d=0}^{d_0-1} \left|S_{d,q}^{(n)}\right| + \frac{1}{M} \sum_{i=1}^{M} A_{d,i} = 2^{n(\log_2(q) - R_2)}, \quad \text{and}$$

$$0 \leq \frac{1}{M} \sum_{i=1}^{M} A_{d_0,i} \leq \left|S_{d_0,q}^{(n)}\right|.$$

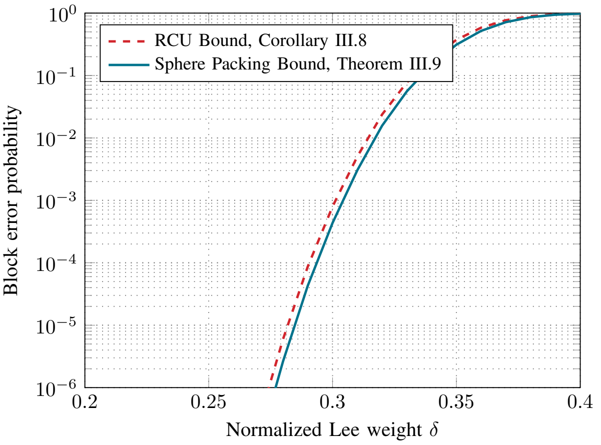

Fig. 2. Random coding union (Corollary III.8) and sphere-packing bounds (Theorem III.9) for the parameters $n = 1024$ and $k = 512$ over $\mathbb{Z}/7\mathbb{Z}$.

Denoting $\xi := \frac{1}{M}\sum_{i=1}^{M} A_{d_0,i}$ and substituting (8) in (7) yields the desired lower bound. □

Figure 2 depicts the random coding union bound of Corollary III.8 and the sphere-packing bound of Theorem III.9, over a memoryless Lee channel, for $[1024, 512]$ codes over $\mathbb{Z}/7\mathbb{Z}$. The random coding union bound given in Corollary III.8 is tight with respect to the sphere-packing bound in Theorem III.9. Hence, they provide an accurate benchmark to assess the performance achievable over the memoryless Lee channel.

## IV. Lee Weight Spectrum of Regular LDPC Code Ensembles

We now turn our attention to regular LDPC code ensembles over $\mathbb{Z}/q\mathbb{Z}$. We are going to derive the average Lee weight spectrum of a random code $\mathcal{C} \subseteq (\mathbb{Z}/q\mathbb{Z})^n$ from the $(d_v, d_c)$ regular LDPC code ensemble. The result will be used in Section V to establish an upper bound on the block error probability under ML decoding.

For each possible Lee weight $\ell \in \{0, \ldots, n\lfloor q/2 \rfloor\}$ we define the number of codewords of Lee weight $\ell$ as

$$W_\ell^{(n)}(\mathcal{C}) := \left|\{\mathbf{c} \in \mathcal{C} \mid \mathrm{wt}_{\mathsf{L}}(\mathbf{c}) = \ell\}\right|.$$

We are now interested in the number of entries of a certain Lee weight in a codeword, i.e., we are interested in the type in terms of the Lee weight of the codeword. For this we introduce the following definition.

**Definition IV.1.** For every codeword $\mathbf{c} \in \mathcal{C}$ we define its *Lee type* to be the $(\lfloor q/2 \rfloor + 1)$-tuple $\boldsymbol{\theta}_{\mathbf{c}} = (\theta_{\mathbf{c}}(0), \ldots, \theta_{\mathbf{c}}(\lfloor q/2 \rfloor))$ consisting of the relative fraction of occurrences of each possible Lee weight $\ell \in \{0, \ldots, \lfloor q/2 \rfloor\}$, i.e.,

$$\theta_{\mathbf{c}}(\ell) = \frac{1}{n}\left|\{k = 1, \ldots, n \mid \mathrm{wt}_{\mathsf{L}}(c_k) = \ell\}\right|.$$

We denote the set of all Lee types over $(\mathbb{Z}/q\mathbb{Z})^n$ by $\mathcal{T}((\mathbb{Z}/q\mathbb{Z})^n)$. Then, we define the number of codewords in a code $\mathcal{C} \subseteq (\mathbb{Z}/q\mathbb{Z})^n$ of Lee type $\boldsymbol{\theta} \in \mathcal{T}((\mathbb{Z}/q\mathbb{Z})^n)$ as

$$A_{\boldsymbol{\theta}}^{(n)}(\mathcal{C}) := \left|\{\mathbf{c} \in \mathcal{C} \mid \boldsymbol{\theta}_{\mathbf{c}} = \boldsymbol{\theta}\}\right|.$$

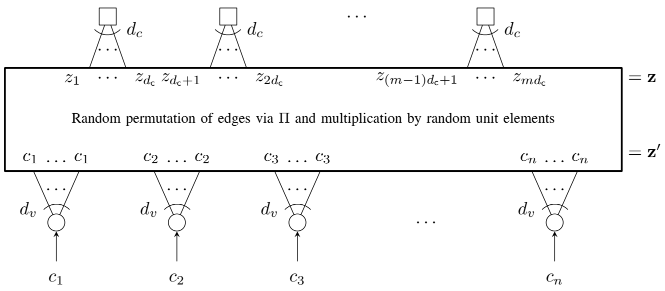
$d_c$
$d_c$
$\cdots$
$d_c$
$z_1$ $\cdots$ $z_{d_c}$ $z_{d_c+1}$ $\cdots$ $z_{2d_c}$
$z_{(m-1)d_c+1}$ $\cdots$ $z_{md_c}$
$= \mathbf{z}$
Random permutation of edges via $\Pi$ and multiplication by random unit elements
$c_1 \ldots c_1$
$c_2 \ldots c_2$
$c_3 \ldots c_3$
$c_n \ldots c_n$
$= \mathbf{z}'$
$d_v$
$d_v$
$d_v$
$\cdots$
$d_v$
$c_1$
$c_2$
$c_3$
$c_n$

Fig. 3. Graphical representation of a random $(d_{\mathsf{v}}, d_{\mathsf{c}})$ LDPC code of length $n$.

Note that we can describe the Lee weight of a codeword $\mathbf{c} \in \mathcal{C}$ in terms of its Lee type as

$$\mathrm{wt}_{\mathsf{L}}(\mathbf{c}) = n \sum_{\ell=1}^{\lfloor q/2 \rfloor} \ell \theta_{\mathbf{c}}(\ell).$$

By abuse of notation, we will call this the *Lee weight of the Lee type* $\boldsymbol{\theta}_{\mathbf{c}}$ and use the notation $\mathrm{wt}_{\mathsf{L}}(\boldsymbol{\theta}_{\mathbf{c}})$. Generally, for a Lee type $\boldsymbol{\theta} \in \mathcal{T}((\mathbb{Z}/q\mathbb{Z})^n)$ we define its Lee weight by $\mathrm{wt}_{\mathsf{L}}(\boldsymbol{\theta}) := n\sum_{\ell=1}^{\lfloor q/2 \rfloor} \ell\theta(\ell)$. Thus, there is a natural relation between $W_\ell^{(n)}(\mathcal{C})$ and $A_{\boldsymbol{\theta}}^{(n)}(\mathcal{C})$. In fact, we have

$$W_\ell^{(n)}(\mathcal{C}) = \sum_{\substack{\boldsymbol{\theta} \in \mathcal{T}((\mathbb{Z}/q\mathbb{Z})^n) \\ \mathrm{wt}_{\mathsf{L}}(\boldsymbol{\theta}) = \ell}} A_{\boldsymbol{\theta}}^{(n)}(\mathcal{C}).$$

In the following, we consider a $(d_v, d_c)$-regular LDPC code $\mathcal{C}$ taken uniformly at random from an ensemble of $(d_v, d_c)$-regular LDPC codes over $\mathbb{Z}/q\mathbb{Z}$. Let $\mathbf{H}$ be a parity-check matrix of $\mathcal{C}$ where the nonzero entries of $\mathbf{H}$ lie in the set of units $(\mathbb{Z}/q\mathbb{Z})^\times$. As $\mathcal{C}$ is a random regular LDPC code, the parity-check matrix $\mathbf{H}$ is a random matrix where each row has $d_c$ nonzero entries taken randomly among the unit elements and each column has $d_v$ of them. We consider a randomly chosen $\mathbf{c} \in (\mathbb{Z}/q\mathbb{Z})^n$ and denote its Lee type by $\boldsymbol{\theta}_{\mathbf{c}}$. Recall that $\mathbf{c}$ is a codeword if and only if $\mathbf{c}\mathbf{H}^\top = \mathbf{0}$.

We now briefly discuss what it means for a codeword $\mathbf{c}$ of a random LDPC code to satisfy the check equations of a parity-check matrix $\mathbf{H}$. Considering the Tanner graph of a code $\mathcal{C}$, given a codeword $\mathbf{c}$ we start by repeating each position $c_i$ exactly $d_{\mathsf{v}}$ times over the edges connected to the $i$-th variable node. We denote the resulting vector by $\mathbf{z}' := (c_1, \ldots, c_1, \ldots, c_n, \ldots, c_n)$. Note that $\mathbf{z}'$ is of length $nd_{\mathsf{v}}$ and is of Lee type $\boldsymbol{\theta}_{\mathbf{z}'} = \boldsymbol{\theta}_{\mathbf{c}}$. Let then $\mathbf{u} \in ((\mathbb{Z}/q\mathbb{Z})^\times)^{nd_{\mathsf{v}}}$ be chosen uniformly at random, i.e., every entry $u_i$ is chosen uniformly at random among the units $(\mathbb{Z}/q\mathbb{Z})^\times$. Finally, choosing a random permutation $\Pi$ we compute $\mathbf{z} := \Pi(\mathbf{z}' \odot \mathbf{u})$. Now, $\mathbf{c}$ satisfies $\mathbf{c}\mathbf{H}^\top = \mathbf{0}$ if and only if $\mathbf{z}$ satisfies the $m$ check equations induced by rows of $\mathbf{H}$. Figure 3 below visualizes this procedure for a random $(d_{\mathsf{v}}, d_{\mathsf{c}})$-regular LDPC code.

Having Figure 3 in mind, we can say that the average Lee type enumerator of a random LDPC code is given by

$$\overline{A}_{\boldsymbol{\theta}}^{(n)} = \binom{n}{n\boldsymbol{\theta}} \mathbb{P}\left(\mathbf{z} \text{ satisfies the check equations} \mid \boldsymbol{\theta}_{\mathbf{c}} = \boldsymbol{\theta}\right).$$

We denote the Lee type of $\mathbf{z}$ by $\boldsymbol{\omega}_{\mathbf{z}}$ in order not to confuse it with the Lee type $\boldsymbol{\theta}_{\mathbf{c}}$. Note that $\boldsymbol{\omega}_{\mathbf{z}}$ highly depends on $\boldsymbol{\theta}_{\mathbf{c}}$. Further discussions and observations follow in Theorem IV.4. For now, let $\mathcal{T}_{\boldsymbol{\theta}_{\mathbf{c}}}\left((\mathbb{Z}/q\mathbb{Z})^{nd_{\mathsf{v}}}\right)$ denote the set of all possible Lee types for a vector $\mathbf{z}$ resulting from the Lee type $\boldsymbol{\theta}_{\mathbf{c}}$. We will denote

$$f^{(n)}(\boldsymbol{\omega}|\boldsymbol{\theta}) := \mathbb{P}\left(\boldsymbol{\omega}_{\mathbf{z}} = \boldsymbol{\omega} | \boldsymbol{\theta}_{\mathbf{c}} = \boldsymbol{\theta}\right) \quad \text{and} \tag{9}$$

$$a^{(n)}(\boldsymbol{\omega}) := \mathbb{P}\left(\mathbf{z} \text{ satisfies the check equations} | \boldsymbol{\omega}_{\mathbf{z}} = \boldsymbol{\omega}\right) \tag{10}$$

Hence, we can further break down the conditional probability as

$$\overline{A}_{\boldsymbol{\theta}}^{(n)} = \binom{n}{n\boldsymbol{\theta}} \sum_{\boldsymbol{\omega} \in \mathcal{T}_{\boldsymbol{\theta}}((\mathbb{Z}/q\mathbb{Z})^{nd_{\mathsf{v}}})} f^{(n)}(\boldsymbol{\omega} \,|\, \boldsymbol{\theta}) a^{(n)}(\boldsymbol{\omega}) \tag{11}$$

In the following we elaborate more the two probabilities $f^{(n)}(\boldsymbol{\omega} \,|\, \boldsymbol{\theta})$ and $a^{(n)}(\boldsymbol{\omega})$.

### A. Transformation of the Lee Type

We start by analyzing how the Lee type of $\mathbf{c}$ changes to the Lee type of the vector $\mathbf{z}$. More precisely, we now study the probability $f^{(n)}(\boldsymbol{\omega} \,|\, \boldsymbol{\theta})$ that the vector $\mathbf{z}$ has a Lee type $\boldsymbol{\omega}_{\mathbf{z}} = \boldsymbol{\omega}$ given that the Lee type of the codeword $\mathbf{c}$ is $\boldsymbol{\theta}_{\mathbf{c}} = \boldsymbol{\theta}$. Recall that $\mathbf{z} \in (\mathbb{Z}/q\mathbb{Z})^{nd_{\mathsf{v}}}$ is formed from $\mathbf{c}$ by repeating the entries $c_i$ each $d_{\mathsf{v}}$ times and then multiplying each copy by a randomly chosen unit. This already implies that the fraction of zeros in $\mathbf{z}$ must be equal to the fraction of zeros in $\mathbf{c}$. Focusing on the nonzero entries of $\mathbf{c}$ we have to treat several cases separately, as the multiplication of a random nonzero element $x \in \mathbb{Z}/q\mathbb{Z}$ by a random unit $u \in (\mathbb{Z}/q\mathbb{Z})^{\times}$ lies in different orbits.

Note that the group of units $(\mathbb{Z}/q\mathbb{Z})^{\times}$ acts under multiplication on $\mathbb{Z}/q\mathbb{Z}$. For an element $a \in \mathbb{Z}/q\mathbb{Z}$ we define its orbit $\mathcal{O}_a$ as

$$\mathcal{O}_a := \left\{a \cdot u \,|\, u \in (\mathbb{Z}/q\mathbb{Z})^{\times}\right\}. \tag{12}$$

Orbits induce an equivalence relation, i.e., two elements are equivalent if and only if they lie within the same orbit. Each orbit can be represented by a divisor of $q$. Let $\mathbb{D}_q$ denote the set of divisors of $q$, i.e.,

$$\mathbb{D}_q := \{\ell \in \mathbb{N} \,:\, \ell \,|\, q\}.$$

Then the distinct orbits are given by $\mathcal{O}_d$ for $d \in \mathbb{D}_q$.

**Example IV.2.** We consider the integer residue ring $\mathbb{Z}/10\mathbb{Z}$. The set of divisors is given by

$$\mathbb{D}_{10} = \{1, 2, 5, 10\}.$$

Hence, there are four orbits defined by the divisors of ten, namely,

$$\mathcal{O}_1 = (\mathbb{Z}/10\mathbb{Z})^{\times} = \{1, 3, 7, 9\}, \ \mathcal{O}_2 = \{2, 4, 6, 8\},$$
$$\mathcal{O}_5 = \{5\} \text{ and } \mathcal{O}_0 := \mathcal{O}_{10} = \{0\}.$$

By the definition of an orbit in (12), we observe that if an element $a$ lies in a given orbit $\mathcal{O}_d$ then every multiple of $a$ by a unit element is in the same orbit. Hence, a codeword $\mathbf{c}$ and a vector $\mathbf{z}$ resulting from $\mathbf{c}$ have the same fraction of elements in an orbit $\mathcal{O}_d$ for every divisor $d \in \mathbb{D}_q$. For a codeword $\mathbf{c}$ with Lee type $\boldsymbol{\theta}_{\mathbf{c}}$ and for every $d \in \mathbb{D}_q$ the fraction of elements in orbit $\mathcal{O}_d$ is denoted as

$$\theta_{\mathbf{c}}(\mathcal{O}_d) := \sum_{\substack{a \in \mathcal{O}_d \\ a \leq \lfloor q/2 \rfloor}} \theta_{\mathbf{c}}(a). \tag{13}$$

The tuple of all such fractions is denoted by

$$\boldsymbol{\theta}_{\mathbf{c},\mathcal{O}} := \left(\theta_{\mathbf{c}}(\mathcal{O}_{d_1}), \ldots, \theta_{\mathbf{c}}(\mathcal{O}_{d_{|\mathbb{D}_q|}})\right).$$

Regarding the Lee metric, we can prove that two elements of the same Lee weight are equivalent.

**Lemma IV.3.** *Elements of the same Lee weight in $\mathbb{Z}/q\mathbb{Z}$ lie in the same orbit, i.e., for every $a \in \mathbb{Z}/q\mathbb{Z}$ we have $\mathcal{O}_a = \mathcal{O}_{q-a}$.*

*Proof.* Let $a \in \mathbb{Z}/q\mathbb{Z}$. By symmetry of the Lee weight, $q - a$ is the only element having the same Lee weight as $a$. Let $b \in \mathcal{O}_{q-a}$ be arbitray. By the definition of an orbit (see Equation (12)), there exists a unit element $u \in (\mathbb{Z}/q\mathbb{Z})^{\times}$ such that $b \equiv u(q-a) \equiv -ua \mod q$. Since $(-1)$ and $u$ are units, also $(-u)$ is a unit modulo $q$ and thus $b \in \mathcal{O}_a$. Since $b$ was chosen arbitrarily, we have $\mathcal{O}_{q-a} = \mathcal{O}_a$. □

Lemma IV.3 indicates that we only have to consider elements up to $\lfloor q/2 \rfloor$. If $q$ is odd, then zero is the only element of Lee weight 0. All other weights in this case are represented by two elements. If instead $q$ is even additionally the Lee weight $\lfloor q/2 \rfloor$ is represented only by one element, namely $\lfloor q/2 \rfloor$ itself. This fact is important when studying the number of configurations of a fixed Lee weight. Given the Lee type $\boldsymbol{\theta}_{\mathbf{x}}$ of a vector $\mathbf{x}$ we denote the fraction of Lee weights with only one representative element by

$$\widehat{\boldsymbol{\theta}}_{\mathbf{x}} := \begin{cases} 1 - \theta_{\mathbf{x}}(0) & \text{if } q \text{ is odd,} \\ 1 - \theta_{\mathbf{x}}(0) - \boldsymbol{\theta}_{\mathbf{x}}(\lfloor q/2 \rfloor). & \text{if } q \text{ is even.} \end{cases}$$

We are then able to state the result on the expression for the probability $f^{(n)}(\boldsymbol{\omega} \,|\, \boldsymbol{\theta})$ over $\mathbb{Z}/q\mathbb{Z}$.

**Theorem IV.4.** *Consider a random $\mathbf{c}$ of Lee type $\boldsymbol{\theta}_c$. Let $\mathbf{z} \in (\mathbb{Z}/q\mathbb{Z})^{nd_{\mathsf{v}}}$ be the resulting vector when repeating the entries of $\mathbf{c}$ $d_{\mathsf{v}}$ times and multiplying each position by a randomly chosen unit element. Furthermore, we denote by $\boldsymbol{\omega}_{\mathbf{z}}$ the Lee type of $\mathbf{z}$ and we define the set*

$$\mathcal{T}_{\boldsymbol{\theta}_{\mathbf{c}}}\left((\mathbb{Z}/q\mathbb{Z})^{nd_{\mathsf{v}}}\right) := \{\boldsymbol{\omega} \in \mathcal{T}((\mathbb{Z}/q\mathbb{Z})^{nd_{\mathsf{v}}}) \,|$$
$$\omega(\mathcal{O}_d) = \theta_{\mathbf{c}}(\mathcal{O}_d) \, \forall d \in \mathbb{D}_q\}.$$

*Let $\mathbb{D}_q = \{d_1, \ldots, d_r\}$ be the set of divisors of $q$. If $\boldsymbol{\omega}_{\mathbf{z}} \in \mathcal{T}_{\boldsymbol{\theta}_{\mathbf{c}}}\left((\mathbb{Z}/q\mathbb{Z})^{nd_{\mathsf{v}}}\right)$, then we have*

$$f^{(n)}(\boldsymbol{\omega}_{\mathbf{z}} \,|\, \boldsymbol{\theta}_{\mathbf{c}}) = \frac{\binom{nd_{\mathsf{v}}}{nd_{\mathsf{v}}\boldsymbol{\omega}_{\mathbf{z}}} 2^{nd_{\mathsf{v}}\widehat{\boldsymbol{\omega}_{\mathbf{z}}}}}{\binom{nd_{\mathsf{v}}}{nd_{\mathsf{v}}\boldsymbol{\theta}_{\mathbf{c},\mathcal{O}}} \prod_{d \in \mathbb{D}_q} |\mathcal{O}_d|^{nd_{\mathsf{v}}\theta_{\mathbf{c}}(\mathcal{O}_d)}} \tag{14}$$

*If not, then the probability $f^{(n)}(\boldsymbol{\omega}_{\mathbf{z}} \,|\, \boldsymbol{\theta}_{\mathbf{c}})$ is zero.*

*Proof.* Assume the Lee type $\boldsymbol{\theta}_{\mathbf{c}}$ of $\mathbf{c}$ is given by $\boldsymbol{\theta}$ and let the Lee type $\boldsymbol{\omega}_{\mathbf{z}}$ be equal to $\boldsymbol{\omega}$. By the above discussion, when multiplying an element $a$ of a given orbit $\mathcal{O}_d$ with a randomly chosen unit $u \in (\mathbb{Z}/d\mathbb{Z})^{\times}$, the product is still an element of $\mathcal{O}_d$. In fact, $au$ can take each element of $\mathcal{O}_d$ with the same probability. Therefore, $\mathbf{z}$ must have the same fraction of elements in orbit $\mathcal{O}_d$ as the codeword $\mathbf{c}$ which also yields, that $f^{(n)}(\boldsymbol{\omega}\,|\,\boldsymbol{\theta}) = 0$ if this is not fulfilled.

Let us assume then that for every divisor $d$ of $q$ it holds that $\omega(\mathcal{O}_d) = \theta(\mathcal{O}_d)$. The probability that $\boldsymbol{\omega}_{\mathbf{z}} = \boldsymbol{\omega}$ given that $\boldsymbol{\theta}_{\mathbf{c}} = \boldsymbol{\theta}$ is given by the number of vectors of length $nd_{\mathsf{v}}$ over $\mathbb{Z}/q\mathbb{Z}$ of Lee type $\boldsymbol{\omega}$ divided by the total number of vectors of a Lee types fulfilling the constraint on the fraction of orbit elements. The number of configurations of vectors with Lee type $\boldsymbol{\omega}$ is given by the multinomial coefficient

$$\binom{nd_{\mathsf{v}}}{nd_{\mathsf{v}}\boldsymbol{\omega}} = \binom{nd_{\mathsf{v}}}{nd_{\mathsf{v}}\omega(0), \dots, nd_{\mathsf{v}}\omega(\lfloor q/2 \rfloor)}.$$

Since the Lee type gives rise only to the number of elements of a certain Lee weight, we must consider Lee weights reached by two different elements. We hence have to multiply the multinomial coefficient by a power of 2 considering the two options for Lee weights admitting two representative elements given by $2^{nd_{\mathsf{v}}\widehat{\omega}}$. This yields us the numerator of the probability $f^{(n)}(\boldsymbol{\omega}\,|\,\boldsymbol{\theta})$ and hence the number of vectors $\mathbf{v} \in (\mathbb{Z}/q\mathbb{Z})^{nd_{\mathsf{v}}}$ of Lee type $\boldsymbol{\omega}$.

We are now interested in finding the number of vectors $\mathbf{v} \in (\mathbb{Z}/q\mathbb{Z})^{nd_{\mathsf{v}}}$ of Lee type $\boldsymbol{\omega}_{\mathbf{v}}$, satisfying $\boldsymbol{\omega}_{\mathbf{v},\mathcal{O}}(\mathcal{O}_d) = \boldsymbol{\theta}_{\mathcal{O}}$. This number splits into two quantities: first, focusing only on the orbits, the number of constellation of the orbits, and second the number of choices in each orbit. The first quantity is again given by a multinomial coefficient regarding the fraction of elements in orbit $\mathcal{O}_d$ for every $d \in \mathbb{D}_q$ given in (13). To obtain the latter quantity we raise the cardinality of the orbit $\mathcal{O}_d$ to the power of the number of positions with elements in that orbit. Combining the results yields the denominator and hence, the desired result on the probability $f^{(n)}(\boldsymbol{\omega}\,|\,\boldsymbol{\theta})$. □

Note that if $q$ is a prime number, there are only two orbits; one containing only the zero element, and one corresponding to the set of units modulo $q$ (which are all nonzero elements). Then the expression in Theorem IV.4 simplifies to

$$f^{(n)}(\boldsymbol{\omega}\,|\,\boldsymbol{\theta}) = \begin{cases} \frac{2^{nd_{\mathsf{v}}\widehat{\omega}}}{(q-1)^{nd_{\mathsf{v}}(1-\theta(0))}} & \text{if } \omega(0) = \theta(0) \\ 0 & \text{otherwise.} \end{cases}$$

Furthermore, there is a closed form for the cardinalities of the orbits which allows for a simple implementation of the formula given in Theorem IV.4.

**Lemma IV.5.** *Let $q$ be a positive integer and let $\mathbb{D}_q$ be the set of divisors of $q$. Furthermore, let $\varphi(\cdot)$ denote the Euler totient function. Then, for every $d \in \mathbb{D}_q$ the cardinality of its orbit is given by*

$$|\mathcal{O}_d| = \varphi(q/d).$$

*Proof.* To compute the cardinality of the orbit $\mathcal{O}_d$, we make use of Lagrange's theorem [30, Theorem 1.8] which yields

$$|\mathcal{O}_d| = \frac{|(\mathbb{Z}/q\mathbb{Z})^{\times}|}{|\mathrm{Stab}(d)|} \tag{15}$$

where $\mathrm{Stab}(d) = \{a \in (\mathbb{Z}/q\mathbb{Z})^{\times} \mid ad = d \mod q\}$ is the stabilizer of $d$. Using that $d\,|\,q$ and the definition of modular equality, we can rewrite $\mathrm{Stab}(d)$ as

$$\begin{aligned} \mathrm{Stab}(d) &= \left\{a \in (\mathbb{Z}/q\mathbb{Z})^{\times} \mid q|(a-1)d\right\} \\ &= \left\{a \in (\mathbb{Z}/q\mathbb{Z})^{\times} \mid (q/d)|(a-1)\right\}. \end{aligned} \tag{16}$$

Since $\mathbb{Z}/q\mathbb{Z}$ is an additive group and since $d\,|\,q$, $d$ is of order $\mathrm{ord}_{\mathbb{Z}/q\mathbb{Z}}(d) = q/d =: D$. Additionally, every element in $\mathcal{O}_d$ is of the same order $D$. Consider now the canonical map $f : (\mathbb{Z}/q\mathbb{Z})^{\times} \longrightarrow (\mathbb{Z}/D\mathbb{Z})^{\times}$ defined by reducing the elements $x \in (\mathbb{Z}/q\mathbb{Z})^{\times}$ modulo $D$. Since $D\,|\,q$, the function $f$ is surjective and therefore, by the fundamental homomorphism theorem [30, Theorem 1.11], we obtain

$$|\ker(f)| = \frac{|(\mathbb{Z}/q\mathbb{Z})^{\times}|}{|(\mathbb{Z}/D\mathbb{Z})^{\times}|} = \frac{\varphi(q)}{\varphi(D)}.$$

Finally, we note that

$$\begin{aligned} \ker(f) &= \left\{a \in (\mathbb{Z}/q\mathbb{Z})^{\times} \mid a-1 = 0 \mod D\right\} \\ &= \left\{a \in (\mathbb{Z}/q\mathbb{Z})^{\times} \mid D|(a-1)\right\} \end{aligned}$$

which corresponds exactly to the stabilizer in (16). Hence, using $|\mathrm{Stab}(d)| = \frac{\varphi(q)}{\varphi(q/d)}$ and $|(\mathbb{Z}/q\mathbb{Z})^{\times}| = \varphi(q)$ in (15) yields the desired result. □

**Example IV.6.** To illustrate (14) presented in Theorem IV.4 consider the following example over $\mathbb{Z}/16\mathbb{Z}$. Note that $\mathbb{Z}/16\mathbb{Z}$ consists of the following five orbits:

$$\mathcal{O}_{16} = \{0\}\,,\ \mathcal{O}_1 = (\mathbb{Z}/16\mathbb{Z})^{\times},\ \mathcal{O}_2 = \{2, 6, 10, 14\}\,,$$
$$\mathcal{O}_4 = \{4, 12\} \text{ and } \mathcal{O}_8 = \{8\}\,.$$

Let $\mathcal{C} \subset (\mathbb{Z}/16\mathbb{Z})^2$ be a regular code with regular variable node degree $d_{\mathsf{v}} = 2$. Let $\mathbf{c} \in \mathcal{C}$ be a codeword of Lee type $\boldsymbol{\theta}_{\mathbf{c}} = (0, 0, 1/2, 0, 1/2, 0, 0, 0, 0)$. Without loss of generality, we can assume that $\mathbf{c} = (2, 4)$. Following the procedure described by Figure 3 yields

$$\mathbf{z}' = (2, 2, 4, 4).$$

When multiplying each of the entries by a randomly chosen unit, we observe that $\mathbf{z}$ can be one of the following vectors (up to permutation and multiplication by $\pm 1$)

$$(2, 2, 4, 4),\ (2, 6, 4, 4), \text{ and } (6, 6, 4, 4).$$

Hence, the possible types for $\mathbf{z}$ are

$$\begin{aligned} \boldsymbol{\omega}^{(1)} &= (0, 0, 1/2, 0, 1/2, 0, 0, 0, 0), \\ \boldsymbol{\omega}^{(2)} &= (0, 0, 1/4, 0, 1/2, 0, 1/4, 0, 0) \text{ and} \\ \boldsymbol{\omega}^{(3)} &= (0, 0, 0, 0, 1/2, 0, 1/2, 0, 0). \end{aligned}$$

The number of permutations for each case is given by the multinomial coefficient with respect to the Lee type $\boldsymbol{\omega}^{(i)}$. For instance, the vector $(2, 2, 4, 4)$ admits 6 permutations, i.e.,

$$\begin{aligned} \binom{nd_{\mathsf{v}}}{nd_{\mathsf{v}}\boldsymbol{\omega}^{(1)}(0), \dots, nd_{\mathsf{v}}\boldsymbol{\omega}^{(1)}(8)} &= \binom{2 \cdot 2}{2 \cdot 2 \cdot (1/2), 2 \cdot 2 \cdot (1/2)} \\ &= \frac{4!}{2!2!} = 6. \end{aligned}$$

Since the Lee type focuses on the Lee weight only and since every nonzero entry different from $\lfloor q/2 \rfloor$ admits two representatives, we have two possible entries for each position. In the case of Lee type $\boldsymbol{\omega}^{(1)}$ we would hence have $6 \cdot 16 = 96$ possible vectors of that type. Similarly, we have 96 vectors of Lee type $\boldsymbol{\omega}^{(3)}$ and 192 vectors of Lee type $\boldsymbol{\omega}^{(2)}$. This yields a total of 384 vectors. Note that this indeed coincides with

$$\begin{aligned}\binom{nd_{\mathsf{v}}}{nd_{\mathsf{v}}\theta_{\mathbf{c}}(\mathcal{O}_1), \ldots, nd_{\mathsf{v}}\theta_{\mathbf{c}}(\mathcal{O}_{16})} \prod_{d \in \mathbb{D}_q} |\mathcal{O}_d|^{nd_{\mathsf{v}}\theta_{\mathbf{c}}(\mathcal{O}_d)} \\ =\binom{4}{2} |\mathcal{O}_2|^2 \, |\mathcal{O}_4|^2 \\ =384.\end{aligned}$$

Thus, the probability that $\mathbf{z}$ has Lee type $\boldsymbol{\omega}^{(1)}$ given that the Lee type of the codeword $\mathbf{c}$ is $\boldsymbol{\theta}_{\mathbf{c}}$ is $f^{(n)}(\boldsymbol{\omega}^{(1)} \mid \boldsymbol{\theta}_{\mathbf{c}}) = \frac{96}{384} = \frac{1}{4}$.

Consequently to Theorem IV.4 we determine the asymptotic growth rate of $f^{(n)}(\boldsymbol{\omega} \mid \boldsymbol{\theta})$ in Corollary IV.7

**Corollary IV.7.** *Let $\mathbf{z} \in (\mathbb{Z}/q\mathbb{Z})^{nd_{\mathsf{v}}}$ be the vector resulting from a vector $\mathbf{c} \in (\mathbb{Z}/q\mathbb{Z})^n$ of Lee type $\boldsymbol{\theta}$ after repetition and permutation. Then we obtain the following asymptotic expression for the probability that $\mathbf{z}$ is of Lee type $\boldsymbol{\omega}$*

$$\begin{aligned}\phi(\boldsymbol{\omega} \mid \boldsymbol{\theta}) :&= \lim_{n \longrightarrow \infty} \frac{1}{n} \log_2(f^{(n)}(\boldsymbol{\omega} \mid \boldsymbol{\theta})) \\ &= d_{\mathsf{v}}\Big(H(\boldsymbol{\omega}) + \widehat{\boldsymbol{\omega}} - H(\boldsymbol{\theta}_{\mathcal{O}}) - \sum_{d \in \mathbb{D}_q} \theta(\mathcal{O}_d) \log_2(|\mathcal{O}_d|)\Big).\end{aligned}$$

*Proof.* The proof follows by taking the limit of each summand. □

Moreover, Lemma IV.8 shows us an even stronger form of convergence.

**Lemma IV.8.** *Given a random regular $(d_{\mathsf{v}}, d_{\mathsf{c}})$ LDPC code over $\mathbb{Z}/q\mathbb{Z}$ and a Lee type $\boldsymbol{\theta} \in \mathcal{T}((\mathbb{Z}/q\mathbb{Z})^n)$. Consider the sequence $f^{(n)}(\boldsymbol{\omega} \mid \boldsymbol{\theta})$ of probabilities, defined in* (14), *with $\boldsymbol{\omega} \in \mathcal{T}_{\boldsymbol{\theta}}\left((\mathbb{Z}/q\mathbb{Z})^{nd_{\mathsf{v}}}\right)$. Then the sequence $\left(\frac{1}{n}\log_2(f^{(n)}(\boldsymbol{\omega} \mid \boldsymbol{\theta}))\right)_{n \in \mathbb{N}}$ is uniformly convergent to $\phi(\boldsymbol{\omega} \mid \boldsymbol{\theta})$ as $n \longrightarrow \infty$.*

*Proof.* We have to show that for every $\varepsilon > 0$ there is a natural number $n_\varepsilon \in \mathbb{N}$ such that for all $n \geq n_\varepsilon$ it holds

$$\left| \frac{1}{n} \log_2(f^{(n)}(\boldsymbol{\omega} \mid \boldsymbol{\theta})) - \phi(\boldsymbol{\omega} \mid \boldsymbol{\theta}) \right| < \varepsilon.$$

Applying Theorem IV.4 and Corollary IV.7, and by using the triangle inequality, we get

$$\begin{aligned}&\left| \frac{1}{n} \log_2(f^{(n)}(\boldsymbol{\omega} \mid \boldsymbol{\theta})) - \phi(\boldsymbol{\omega} \mid \boldsymbol{\theta}) \right| \\ &= \Bigg| \frac{1}{n} \log_2 \left( \tbinom{nd_{\mathsf{v}}}{nd_{\mathsf{v}}\boldsymbol{\omega}} \right) - d_{\mathsf{v}} H(\boldsymbol{\omega}) \\ &\qquad - \frac{1}{n} \log_2 \left( \tbinom{nd_{\mathsf{v}}}{nd_{\mathsf{v}}\boldsymbol{\theta}_{\mathcal{O}}} \right) + d_{\mathsf{v}} H(\boldsymbol{\theta}_{\mathcal{O}}) \Bigg| \\ &\leq \left| \frac{1}{n} \log_2 \left( \tbinom{nd_{\mathsf{v}}}{nd_{\mathsf{v}}\boldsymbol{\omega}} \right) - d_{\mathsf{v}} H(\boldsymbol{\omega}) \right| \\ &\qquad + \left| d_{\mathsf{v}} H(\boldsymbol{\theta}_{\mathcal{O}}) - \frac{1}{n} \log_2 \left( \tbinom{nd_{\mathsf{v}}}{nd_{\mathsf{v}}\boldsymbol{\theta}_{\mathcal{O}}} \right) \right|.\end{aligned}$$

Let us focus now on $\left| \frac{1}{n} \log_2 \left( \tbinom{nd_{\mathsf{v}}}{nd_{\mathsf{v}}\boldsymbol{\omega}} \right) - d_{\mathsf{v}} H(\boldsymbol{\omega}) \right|$. Recall from (3) that we have the following bounds on $\binom{nd_{\mathsf{v}}}{nd_{\mathsf{v}}\boldsymbol{\omega}}$,

$$\frac{1}{(nd_{\mathsf{v}} + 1)^{\lfloor q/2 \rfloor + 1}} 2^{nd_{\mathsf{v}} H(\boldsymbol{\omega})} \leq \binom{nd_{\mathsf{v}}}{nd_{\mathsf{v}}\boldsymbol{\omega}} \leq 2^{nd_{\mathsf{v}} H(\boldsymbol{\omega})}.$$

Hence, if $\frac{1}{n} \log_2 \left( \tbinom{nd_{\mathsf{v}}}{nd_{\mathsf{v}}\boldsymbol{\omega}} \right) > d_{\mathsf{v}} H(\boldsymbol{\omega})$, we get

$$\left| \frac{1}{n} \log_2 \left( \binom{nd_{\mathsf{v}}}{nd_{\mathsf{v}}\boldsymbol{\omega}} \right) - d_{\mathsf{v}} H(\boldsymbol{\omega}) \right| = 0.$$

On the other hand, we obtain

$$\begin{aligned}&\left| \frac{1}{n} \log_2 \left( \tbinom{nd_{\mathsf{v}}}{nd_{\mathsf{v}}\boldsymbol{\omega}} \right) - d_{\mathsf{v}} H(\boldsymbol{\omega}) \right| \\ &\qquad \leq (\lfloor q/2 \rfloor + 1) \frac{1}{n} \log_2 (nd_{\mathsf{v}} + 1).\end{aligned}$$

By l'Hôpital's rule this converges to zero as $n$ tends to $\infty$.

Note that the same argument holds for $\Big| d_{\mathsf{v}} H(\boldsymbol{\theta}_{\mathcal{O}}) - \frac{1}{n} \log_2 \left( \tbinom{nd_{\mathsf{v}}}{nd_{\mathsf{v}}\boldsymbol{\theta}_{\mathcal{O}}} \right) \Big|$ and thus the result follows. □

### *B. Valid Check Node Assignments*

We now discuss the probability $a^{(n)}(\boldsymbol{\omega})$ given in (10). We make use of generating functions to describe the situation at one check node and then extend the generating function to $m$ check nodes. In the following let $w$ denote the Lee weight decomposition of a vector $\mathbf{x} \in (\mathbb{Z}/q\mathbb{Z})^n$. That is, for every $i = 0, \ldots, \lfloor q/2 \rfloor$,

$$w_i = \left| \{ k = 1, \ldots, n \mid \mathrm{wt}_{\mathsf{L}}(x_k) = i \} \right|.$$

Furthermore, recall from Equation (14) in Theorem IV.4 that given a Lee type $\boldsymbol{\theta}$ of $\mathbf{c}$, the Lee type $\boldsymbol{\omega}$ of a valid check node assignment has to show the same orbit distribution. Hence, there is a restricted choice. Let us denote the set of possible check node types resulting from $\boldsymbol{\theta}$ by $\mathcal{T}_{\boldsymbol{\theta}}\left((\mathbb{Z}/q\mathbb{Z})^{nd_{\mathsf{v}}}\right)$, i.e., it is the set

$$\left\{ \boldsymbol{\omega} \in \mathcal{T}((\mathbb{Z}/q\mathbb{Z})^{nd_{\mathsf{v}}}) \mid \omega(\mathcal{O}_d) = \theta(\mathcal{O}_d) \, \forall d \in \mathbb{D}_q \right\}.$$

In the following, for a given polynomial $p(x)$, we denote by $\mathrm{coeff}(p(x), x^i)$ the coefficient of $x^i$ in $p(x)$.

**Theorem IV.9.** *Consider a vector $\mathbf{z} \in (\mathbb{Z}/q\mathbb{Z})^{nd_{\mathsf{v}}}$ of Lee type $\boldsymbol{\omega}$ and weight decomposition $w$. Furthermore, consider a random regular LDPC code of variable degree $d_{\mathsf{v}}$ and check node degree $d_{\mathsf{c}}$. Then, the probability that $\mathbf{z}$ fulfills the check node equations is given by*

$$a^{(n)}(\boldsymbol{\omega}) = \frac{\mathrm{coeff}(G(\mathbf{t}), \mathbf{t}^{\boldsymbol{\omega} nd_{\mathsf{v}}})}{\binom{nd_{\mathsf{v}}}{nd_{\mathsf{v}}\boldsymbol{\omega}}},$$

*where*

$$G(\mathbf{t}) = \tfrac{1}{q^m} \left[ \sum_{\substack{\mathbf{z}_i \in (\mathbb{Z}/q\mathbb{Z})^{d_{\mathsf{c}}} \\ d_{\mathsf{c}}\boldsymbol{\omega}_{\mathbf{z}_i} = w}} \sum_{s=0}^{q-1} \prod_{k=1}^{d_{\mathsf{c}}} \mathrm{e}^{\frac{2\pi i}{q} s z_k} t_1^{nd_{\mathsf{v}}\boldsymbol{\omega}(1)} \ldots t_{\lfloor q/2 \rfloor}^{nd_{\mathsf{v}}\omega(\lfloor q/2 \rfloor)} \right]^m.$$

*Proof.* Recall that $a^{(n)}(\boldsymbol{\omega})$ describes the probability of $\mathbf{z} \in (\mathbb{Z}/q\mathbb{Z})^{nd_{\mathsf{v}}}$ satisfying the check node equations and being of a given Lee type $\boldsymbol{\omega}$. Furthermore, we have $m$ check nodes each of degree $d_{\mathsf{c}}$. Hence, we can split $\mathbf{z}$ into $m$ parts $\mathbf{z}_1, \dots, \mathbf{z}_m$ each one corresponding check node $\mathsf{c}_1, \dots, \mathsf{c}_m$, respectively.

We focus now on one check node only and describe a generating function for the number of $\mathbf{z}_i$'s satisfying the check node equations of check node $\mathsf{c}_i$ and having Lee weight decomposition given by $w = (w_0, \dots, w_{\lfloor q/2 \rfloor})$. We turn our attention at this point only to the nonzero elements and note that $w_0 = d_{\mathsf{c}} - \sum_{i=1}^{\lfloor q/2 \rfloor} w_i$. In that sense, let us define

$$g_{(w_1,\dots,w_{\lfloor q/2 \rfloor})} := \Big| \Big\{ \mathbf{z}_i \in (\mathbb{Z}/q\mathbb{Z})^{d_{\mathsf{c}}} \Big| \mathbf{z}_i \text{ satisfies the check-eq.,} \\ \big| \{ j = 1, \dots, d_{\mathsf{c}} \mid \mathrm{wt}_{\mathsf{L}}(z_{i_j}) = k \} \big| = w_k \Big\} \Big|.$$

We can describe this quantity summing over all $d_{\mathsf{c}}$-tuples that sum up to zero using an indicator function. Indeed,

$$g_{(w_1,\dots,w_{\lfloor q/2 \rfloor})} = \sum_{\substack{\mathbf{z}_i \in (\mathbb{Z}/q\mathbb{Z})^{d_{\mathsf{c}}} \\ d_{\mathsf{c}} \boldsymbol{\omega}_{\mathbf{z}_i} = w}} \mathbb{1} \left( \sum_{k=1}^{d_{\mathsf{c}}} z_k = 0 \right).$$

Applying the inversion formula for the discrete Fourier transform over $\mathbb{Z}/q\mathbb{Z}$ yields

$$g_{(w_1,\dots,w_{\lfloor q/2 \rfloor})} = \sum_{\substack{\mathbf{z}_i \in (\mathbb{Z}/q\mathbb{Z})^{d_{\mathsf{c}}} \\ d_{\mathsf{c}} \boldsymbol{\omega}_{\mathbf{z}_i} = w}} \frac{1}{q} \sum_{\chi \text{ character}} \chi \left( \sum_{k=1}^{d_{\mathsf{c}}} z_k \right). \tag{17}$$

Over the finite abelian group $\mathbb{Z}/q\mathbb{Z}$ there are $q$ characters $\chi_0, \dots, \chi_{q-1}$ defined by $\chi_k(a) := \mathrm{e}^{\frac{2\pi i}{q} ka}$ for each element $a \in \mathbb{Z}/q\mathbb{Z}$. Hence, we can rewrite (17) as

$$g_{(w_1,\dots,w_{\lfloor q/2 \rfloor})} = \frac{1}{q} \sum_{\substack{\mathbf{z}_i \in (\mathbb{Z}/q\mathbb{Z})^{d_{\mathsf{c}}} \\ d_{\mathsf{c}} \boldsymbol{\omega}_{\mathbf{z}_i} = w}} \sum_{s=0}^{q-1} \mathrm{e}^{\frac{2\pi i}{q} s \sum_{k=1}^{d_{\mathsf{c}}} z_k}. \tag{18}$$

We then define the generating function $g(\mathbf{t})$ by

$$g(\mathbf{t}) := \sum_{\substack{w \text{ composition} \\ \text{of } d_{\mathsf{c}}}} g_{(w_1,\dots,w_{\lfloor q/2 \rfloor})} t_1^{w_1} \dots t_{\lfloor q/2 \rfloor}^{w_{\lfloor q/2 \rfloor}}.$$

To obtain a similar expression for a configuration regarding all the check nodes, we take the $m$-fold convolution of $g_{(w_1,\dots,w_{\lfloor q/2 \rfloor})}$, i.e.,

$$G_{(w_1,\dots,w_{\lfloor q/2 \rfloor})} := g_{(w_1,\dots,w_{\lfloor q/2 \rfloor})} \circledast \dots \circledast g_{(w_1,\dots,w_{\lfloor q/2 \rfloor})}.$$

Hence, the corresponding generating function for $m$ check nodes is

$$\begin{aligned} G(\mathbf{t}) &:= \sum_{\substack{w \text{ composition} \\ \text{of } md_{\mathsf{c}}}} g_{(w_1,\dots,w_{\lfloor q/2 \rfloor})} t_1^{w_1} \dots t_{\lfloor q/2 \rfloor}^{w_{\lfloor q/2 \rfloor}} \\ &= g(\mathbf{t})^m. \end{aligned}$$

Let $\boldsymbol{\omega}$ denote the Lee type of the decomposition $w$, i.e., $nd_{\mathsf{v}}\omega(i) = w_i$ for every $i \in \{0, \dots, \lfloor q/2 \rfloor\}$. The number of configurations of given Lee type $\boldsymbol{\omega}$ is then the coefficient of the polynomial $G(\mathbf{t})$ at $\mathbf{t}^{nd_{\mathsf{v}}\boldsymbol{\omega}} = t_1^{w_1} \dots t_{\lfloor q/2 \rfloor}^{w_{\lfloor q/2 \rfloor}}$. Finally, the probability $a^{(n)}(\boldsymbol{\omega})$ is obtained by dividing the $nd_{\mathsf{v}}\boldsymbol{\omega}$-th coefficient of $G(\mathbf{t})$ by all the possible permutations of a vector $\mathbf{x} \in (\mathbb{Z}/q\mathbb{Z})^{nd_{\mathsf{v}}}$ of Lee type $\boldsymbol{\omega}$, which is given by the multinomial coefficient $\binom{nd_{\mathsf{v}}}{nd_{\mathsf{v}}\boldsymbol{\omega}}$. □

At this point, to simplify the understanding we would like to discuss the expression in (18) with an example.

**Example IV.10.** Assume the check node degree is $d_{\mathsf{c}} = 2$ and that the underlying integer ring is $\mathbb{Z}/5\mathbb{Z}$. Let us furthermore assume that the Lee weight decomposition of a tuple $\mathbf{z}_i$ at a check node is $w = (0, 2, 0)$. This means that $\mathbf{z}_i$ is one of the following tuples

$$(1,1), \quad (1,4), \quad (4,1), \quad \text{or} \quad (4,4).$$

Since only $(1,4)$ and $(4,1)$ satisfy the check equation (i.e. sum up to zero modulo five), the enumerator $g_{(0,2,0)}$ should equal two. In fact, the exponential expression in Equation (18) equals $1$ for all tuples satisfying the check equation. For those not satisfying the check equation the sum of exponentials is the sum of $n$-th roots of unity (in our case $n = 5$) and is hence equal to zero.

Let us now focus on the asymptotic growth rate of $a^{(n)}$ which we define as

$$\alpha(\boldsymbol{\omega}) := \lim_{n \longrightarrow \infty} \frac{1}{n} \log_2(a^{(n)}(\boldsymbol{\omega})).$$

A direct consequence of taking the logarithm and the limit of the sequence $a^{(n)}$ is captured in Corollary IV.11.

**Corollary IV.11.** *Let $\mathbf{z} \in (\mathbb{Z}/q\mathbb{Z})^{nd_{\mathsf{v}}}$ satisfy the $m$ check equations and denote by $\boldsymbol{\omega}$ its Lee type. Then we obtain the following asymptotic expression for the probability $a^{(n)}(\boldsymbol{\omega})$.*

$$\alpha(\boldsymbol{\omega}) = -d_{\mathsf{v}} H(\boldsymbol{\omega}) + (1 - R) \inf_{\mathbf{t} \succ 0} \log_2 \left( \frac{g(\mathbf{t})}{\mathbf{t}^{\boldsymbol{\omega} nd_{\mathsf{v}}}} \right),$$

*where $\mathbf{t} \succ 0$ means that not every entry of $\mathbf{t} = (t_1, \dots, t_{\lfloor q/2 \rfloor})$ is equal to zero.*

Taking the infimum over all possibilities of $\mathbf{t} = (t_1, \dots, t_{\lfloor q/2 \rfloor})$ is impractical. We will use the asymptotic Hayman method for multivariate polynomials (see [31], [32], [33]) to establish $\lim_{n \longrightarrow \infty} 1/n \log_2 \left( \mathrm{coeff}(G(\mathbf{t}), \mathbf{t}^{\boldsymbol{\omega} nd_{\mathsf{v}}} \right)$.

**Lemma IV.12** (Hayman Formula). *Let $\mathbf{x} = (x_1, \dots, x_d) \in \mathbb{R}^d$ and let $p(\mathbf{x})$ be a multivariate polynomial with $p(\mathbf{0}) \neq 0$. Furthermore, let $\boldsymbol{\beta} = (\beta_1, \dots, \beta_d)$ such that $0 \leq \beta_i \leq 1$ and $\beta_i n \in \mathbb{N}$ for all $i = 1, \dots, d$. Assume that $\mathbf{x}^\star = (x_1^\star, \dots, x_d^\star)$ is the unique positive real solution to the system of equations given by*

$$x_1 \frac{\partial p(\mathbf{x})}{\partial x_1} = \beta_1 p(\mathbf{x}), \ \dots, \ x_d \frac{\partial p(\mathbf{x})}{\partial x_d} = \beta_d p(\mathbf{x}).$$

*Then, as $n \longrightarrow \infty$, it holds*

$$\begin{aligned} &\lim_{n \longrightarrow \infty} \frac{1}{n} \ln \left( \mathrm{coeff} \left( (p(\mathbf{z}))^n, \mathbf{z}^{n\beta} \right) \right) \\ &\quad = \left( \ln(p(\mathbf{x})) - \sum_{i=1}^{d} \beta_i \ln(x_i) \right). \end{aligned}$$

In our case, we have that

$$\begin{aligned} &\lim_{n \longrightarrow \infty} \frac{1}{n} \ln \left( \mathrm{coeff} \left( (g(\mathbf{t})^{1/d_{\mathsf{c}}})^{nd_{\mathsf{v}}}, \mathbf{t}^{\boldsymbol{\omega} nd_{\mathsf{v}}} \right) \right) \\ &\quad = d_{\mathsf{v}} \lim_{n' \longrightarrow \infty} \frac{1}{n'} \ln \left( \mathrm{coeff} \left( (g(\mathbf{t})^{1/d_{\mathsf{c}}})^{n'}, \mathbf{t}^{\boldsymbol{\omega} n'} \right) \right). \end{aligned}$$

Hence, Corollary IV.13 is a direct consequence of Hayman's Formula.

**Corollary IV.13.** *Let $\boldsymbol{\omega} = (\omega(0), \dots, \omega(\lfloor q/2 \rfloor)) \in (0,1)^{\lfloor q/2 \rfloor + 1}$ such that $\omega(i) n d_{\mathsf{v}} \in \mathbb{N}$ for every $i = 1, \dots, d$. Then*

$$\alpha(\boldsymbol{\omega}) = d_{\mathsf{v}} \left( H(\boldsymbol{\omega}) + \log_2 \left( g(\mathbf{t}^\star)^{1/d_{\mathsf{c}}} \right) - \sum_{i=1}^{\lfloor q/2 \rfloor} \omega(i) \log_2(t_i^\star) \right)$$

*where $\mathbf{t}^\star = (t_1^\star, \dots, t_{\lfloor q/2 \rfloor}^\star)$ is the unique positive real solution to the equations*

$$t_i \frac{\partial g(\mathbf{t})^{1/d_{\mathsf{c}}}}{\partial t_i} = \omega(i) g(\mathbf{t})^{1/d_{\mathsf{c}}}, \quad i = 1, \dots, \lfloor q/2 \rfloor.$$

In his paper, Hayman gave an explicit expression for the coefficient of an admissible function (see [31, p. 69]). With this, it easily follows that the sequence of functions $\left(\frac{1}{n} \log_2(a^{(n)})\right)_{n \in \mathbb{N}}$ is uniformly convergent.

### C. Asymptotic Growth Rate

Having determined the two probabilities defined in Equations (9) and (10), respectively, the expression for the average Lee type enumerator $\overline{A}_{\boldsymbol{\theta}}^{(n)}$ follows immediately. We can then deduce immediately the asymptotics of the average Lee type enumerator and average weight enumerator, respectively.

**Corollary IV.14.** *Let $\mathcal{C}$ be a random $(d_{\mathsf{v}}, d_{\mathsf{c}})$-regular LDPC code of length $n$ over $\mathbb{Z}/q\mathbb{Z}$. Let us denote by $\mathcal{A}(\boldsymbol{\theta}) := \lim_{n \longrightarrow \infty} \frac{1}{n} \log_2 \overline{A}_{\boldsymbol{\theta}}^{(n)}$ and $\mathcal{W}(\ell) := \lim_{n \longrightarrow \infty} \frac{1}{n} \log_2 \overline{W}_{\ell}^{(n)}$ the spectral growth rate of the average Lee type enumerator and weight enumerator, respectively. Then*

$$\mathcal{A}(\boldsymbol{\theta}) \leq H(\boldsymbol{\theta}) + \sup_{\boldsymbol{\omega} \in \mathcal{T}_{\boldsymbol{\theta}}((\mathbb{Z}/q\mathbb{Z})^{n d_{\mathsf{v}}})} \left( \phi(\boldsymbol{\omega} \mid \boldsymbol{\theta}) + \alpha(\boldsymbol{\omega}) \right)$$

*and, in particular,*

$$\mathcal{W}(\ell) \leq \sup_{\substack{\boldsymbol{\theta} \in \mathcal{T}((\mathbb{Z}/q\mathbb{Z})^n) \\ \mathrm{wt}_{\mathsf{L}}(\boldsymbol{\theta}) = \ell}} \mathcal{A}(\boldsymbol{\theta}). \tag{19}$$

*Proof.* From Equation (11) we observe that

$$\bar{A}_{\boldsymbol{\theta}}^{(n)} = \binom{n}{n\boldsymbol{\theta}} \sum_{\boldsymbol{\omega} \in \mathcal{T}_{\boldsymbol{\theta}}((\mathbb{Z}/q\mathbb{Z})^{n d_{\mathsf{v}}})} f^{(n)}(\boldsymbol{\omega} \mid \boldsymbol{\theta}) a^{(n)}(\boldsymbol{\omega})$$

and hence

$$\mathcal{A}(\boldsymbol{\theta}) = H(\boldsymbol{\theta}) + \lim_{n \longrightarrow \infty} \frac{1}{n} \log_2 \left( \sum_{\substack{\boldsymbol{\omega} \in \\ \mathcal{T}_{\boldsymbol{\theta}}\left((\mathbb{Z}/q\mathbb{Z})^{n d_{\mathsf{v}}}\right)}} f^{(n)}(\boldsymbol{\omega} | \boldsymbol{\theta}) a^{(n)}(\boldsymbol{\omega}) \right).$$

Furthermore, we can write

$$\begin{aligned}
&\frac{1}{n} \log_2 \left( \sum_{\boldsymbol{\omega} \in \mathcal{T}_{\boldsymbol{\theta}}((\mathbb{Z}/q\mathbb{Z})^{n d_{\mathsf{v}}})} f^{(n)}(\boldsymbol{\omega} \mid \boldsymbol{\theta}) a^{(n)}(\boldsymbol{\omega}) \right) \\
&\leq \frac{1}{n} \log_2 \left( \sup_{\boldsymbol{\omega} \in \mathcal{T}_{\boldsymbol{\theta}}((\mathbb{Z}/q\mathbb{Z})^{n d_{\mathsf{v}}})} \left[ f^{(n)}(\boldsymbol{\omega} \mid \boldsymbol{\theta}) a^{(n)}(\boldsymbol{\omega}) \right] \right. \\
&\qquad\qquad \left. \cdot \left| \mathcal{T}_{\boldsymbol{\theta}} \left( (\mathbb{Z}/q\mathbb{Z})^{n d_{\mathsf{v}}} \right) \right| \right) \\
&\overset{(a)}{=} \sup_{\substack{\boldsymbol{\omega} \in \\ \mathcal{T}_{\boldsymbol{\theta}}\left((\mathbb{Z}/q\mathbb{Z})^{n d_{\mathsf{v}}}\right)}} \left[ \frac{1}{n} \log_2 \left( f^{(n)}(\boldsymbol{\omega} \mid \boldsymbol{\theta}) a^{(n)}(\boldsymbol{\omega}) \right) \right] \\
&= \sup_{\substack{\boldsymbol{\omega} \in \\ \mathcal{T}_{\boldsymbol{\theta}}\left((\mathbb{Z}/q\mathbb{Z})^{n d_{\mathsf{v}}}\right)}} \left[ \frac{1}{n} \log_2 \left( f^{(n)}(\boldsymbol{\omega} \mid \boldsymbol{\theta}) \right) + \frac{1}{n} \log_2 \left( a^{(n)}(\boldsymbol{\omega}) \right) \right]
\end{aligned}$$

where for $(a)$ we used, that $\left| \mathcal{T}_{\boldsymbol{\theta}} \left( (\mathbb{Z}/q\mathbb{Z})^{n d_{\mathsf{v}}} \right) \right|$ is polynomial in $n$. By the uniform convergence shown in Lemma IV.8 and in [31], we can switch the limit with the supremum and the statement follows. The bound in (19) for $\mathcal{W}(\ell)$ follows in an analogous manner. □

Figures 4, 5 and 6 show the spectral growth rate of the average weight enumerator of a random regular $(3,6)$ LDPC code over $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$, respectively, and compare it to the spectral growth rate of a random code $\mathcal{C} \subset (\mathbb{Z}/q\mathbb{Z})^n$ of the same rate $R$. Note that, for a random code $\mathcal{C}$, the average Lee weight enumerator $\overline{W}_{\ell}^{(n)}(\mathcal{C})$, for every $\ell \in \{0, \dots, n\lfloor q/2 \rfloor\}$ is computed as

$$\overline{W}_{\ell}^{(n)}(\mathcal{C}) = |\mathcal{C}| \, \mathbb{P}(\mathrm{wt}_{\mathsf{L}}(\mathbf{x}) = \ell)$$

Taking logarithms and limits on both sides, and defining $\delta = \ell/n$ yields

$$\begin{aligned}
\mathcal{W}(\delta n) &= \lim_{n \longrightarrow \infty} \frac{1}{n} \log_2 \left( |\mathcal{C}| \right) \\
&\quad + \lim_{n \longrightarrow \infty} \frac{1}{n} \log_2 \left( \mathbb{P}(\mathrm{wt}_{\mathsf{L}}(\mathbf{x}) = \delta n) \right) \\
&= R_2 + \lim_{n \longrightarrow \infty} \frac{1}{n} \log_2 \left( \mathbb{P}(\mathbf{x} \in S_{\delta n, q}^{(n)}) \right) \\
&= R_2 + \lim_{n \longrightarrow \infty} \frac{1}{n} \log_2 \left( \frac{\left| S_{\delta n, q}^{(n)} \right|}{q^n} \right) \\
&= R_2 - \log_2(q) + H(B_\delta).
\end{aligned}$$

## V. Performance Analysis of LDPC Codes over the Lee Channels

In this section, we analyze the error-correction performance of regular LDPC codes over the two channel models presented in Section II-E. First and foremost, we discuss an upper bound on the block error probability under ML decoding over the memoryless Lee channel using a union bound argument. We then focus on the performance with respect to the BP decoder and the SMP decoder, respectively. For both decoders we start by adapting the decoders to the Lee metric over integer residue rings discussing the main changes and assumptions needed for providing a full density evolution analysis.

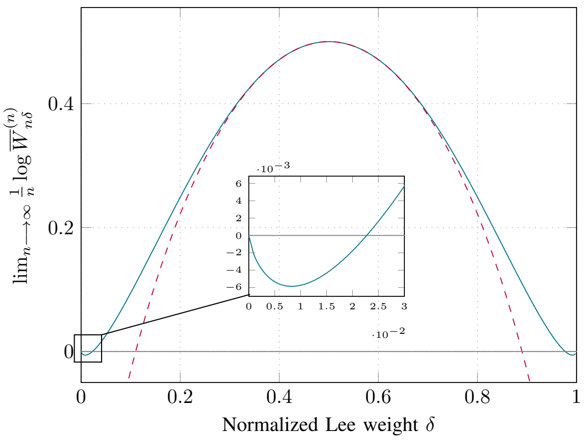

Fig. 4. Spectral growth rate of the average weight enumerator of a regular $(3, 6)$ LDPC code ensembles over $\mathbb{Z}/2\mathbb{Z}$ (solid blue line) versus the spectral growth rate of the average weight enumerator of a random code over $\mathbb{Z}/2\mathbb{Z}$ and rate $R = 1/2$ (dashed red line). The logarithm is in base $q$.

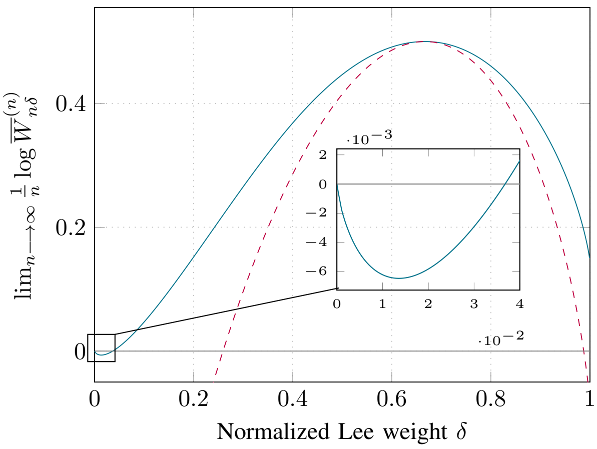

Fig. 5. Spectral growth rate of the average weight enumerator of a regular $(3, 6)$ LDPC code ensembles over $\mathbb{Z}/3\mathbb{Z}$ (solid blue line) versus the spectral growth rate of the average weight enumerator of a random code over $\mathbb{Z}/3\mathbb{Z}$ and rate $R = 1/2$ (dashed red line). The logarithm is in base $q$.

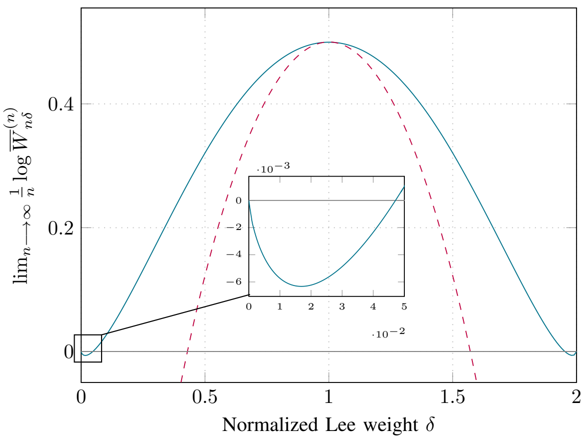

Fig. 6. Spectral growth rate of the average weight enumerator of a regular $(3, 6)$ LDPC code ensembles over $\mathbb{Z}/4\mathbb{Z}$ (solid blue line) versus the spectral growth rate of the average weight enumerator of a random code over $\mathbb{Z}/4\mathbb{Z}$ and rate $R = 1/2$ (dashed red line). The logarithm is in base $q$.

### *A. Bounds on the Block Error Probability Based on the Lee Weight Spectrum*

We are interested in the average block error probability under ML decoding of random regular LDPC code ensembles over $\mathbb{Z}/q\mathbb{Z}$ in the memoryless Lee channel. As the channel is symmetric, we can assume the transmission of the zero codeword. The ML decoder fails if and only if there is a nonzero codeword $\mathbf{c} \in \mathcal{C} \setminus \{\mathbf{0}\}$ satisfying

$$P_{\mathbf{Y}\,|\,\mathbf{X}}(\mathbf{y}\,|\,\mathbf{0}) \leq P_{\mathbf{Y}\,|\,\mathbf{X}}(\mathbf{y}\,|\,\mathbf{c}).$$

We refer to the probability of this event as the pairwise error probability and denote it by $\mathsf{PEP}(\mathbf{0} \to \mathbf{c})$. Note that in the spirit of obtaining an upper bound on the block error probability, we break ties always in favor of the erroneous codeword. Using a union bound argument, we observe that the block error probability is upper bounded by the sum of all pairwise error probabilities, i.e.,

$$P_B(\mathcal{C}) \leq \sum_{\mathbf{c}\in\mathcal{C}\setminus\{\mathbf{0}\}} \mathsf{PEP}(\mathbf{0} \to \mathbf{c}). \tag{20}$$

We can rewrite the pairwise error probability as

$$\mathsf{PEP}(\mathbf{0} \to \mathbf{c}) = \mathbb{P}\left(\frac{P_{\mathbf{Y}\,|\,\mathbf{X}}(\mathbf{y}\,|\,\mathbf{0})}{P_{\mathbf{Y}\,|\,\mathbf{X}}(\mathbf{y}\,|\,\mathbf{c})} \leq 1\right). \tag{21}$$

Denoting the log-likelihood ratio as

$$\Lambda(y, c) := \log\left(\frac{P_{Y\,|\,X}(y\,|\,0)}{P_{Y\,|\,X}(y\,|\,c)}\right)$$

we have $\mathsf{PEP}(\mathbf{0} \to \mathbf{c}) = \mathbb{P}\left(\sum_{i=1}^{n} \Lambda(y_i, c_i) \leq 0\right)$. Hence, the analysis reduces to the analysis of the distribution of the random variables $\Lambda_\ell := \Lambda(Y, c = \ell)$, where $Y$ is a random variable distributed as $B_\delta$. Owing to the symmetry of the Boltzmann distribution, we have that

$$P_{Y\,|\,X}(y\,|\,c) = P_{Y\,|\,X}(-y\,|\,-c)$$

and therefore also

$$\Lambda(y, c = \ell) = \Lambda(-y, c = -\ell).$$

It follows that the distribution of $\Lambda_\ell$ equals the distribution of $\Lambda_{-\ell}$. Hence, the evaluation of (21) can be carried out by counting the number of elements in $\mathbf{c}$ possessing Lee weight $\ell$ with $\ell \in \{0, \dots \lfloor q/2 \rfloor\}$. We will therefore again make use of the Lee type of a codeword (see Definition IV.1). Thus, we can rewrite the pairwise error probability for any nonzero codeword $\mathbf{c} \in \mathcal{C} \setminus \{0\}$ as follows

$$\mathsf{PEP}(\mathbf{0} \to \mathbf{c}) = \mathbb{P}\left(\sum_{\ell=1}^{\lfloor q/2 \rfloor} \sum_{j=1}^{n\theta_{\mathbf{c}}(\ell)} \Lambda_j \leq 0\right).$$

This gives us an exact value of the pairwise error probability under ML decoding. However, this expression requires eventually to iterate over every Lee type in the code $\mathcal{C}$ and is therefore inefficient for codes with large parameters. In the following we present a "worst case" candidate for the pairwise error probability which ultimately serves to upper bound the block error probability.

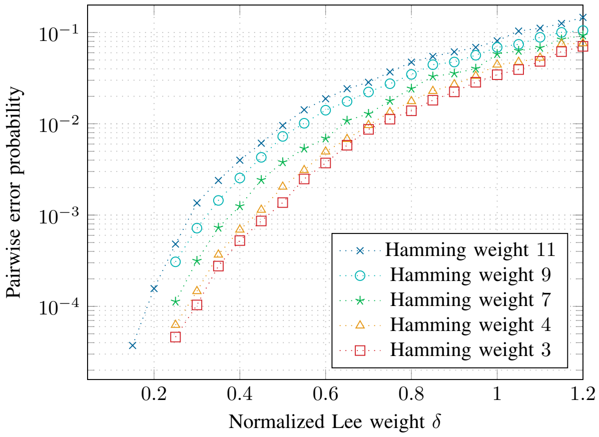

Fig. 7. Comparison of the pairwise error probabilities over $\mathbb{Z}/9\mathbb{Z}$ of vectors of Lee weight 11 and varying Hamming weight.

**Lemma V.1.** *Consider a nonzero codeword* $\mathbf{c} \in \mathcal{C}$ *such that* $\mathrm{wt}_{\mathsf{L}}(\mathbf{c}) = t$. *Let* $\mathbf{x}_{|_t} \in (\mathbb{Z}/q\mathbb{Z})^n$ *be of Lee type* $\boldsymbol{\theta}_{\mathbf{x}_{|_t}} = (1 - t/n, t/n, 0, \dots, 0)$. *Over a memoryless Lee channel with* $\delta \leq \delta_q$ *we have*

$$\mathsf{PEP}(\mathbf{0} \to \mathbf{c}) \leq \mathsf{PEP}(\mathbf{0} \to \mathbf{x}_{|_t})$$

*where equality holds if and only if* $\mathbf{c}$ *is of the same Lee type* $\boldsymbol{\theta}_{\mathbf{c}} = \boldsymbol{\theta}_{\mathbf{x}_{|_t}}$.

Observe that the nonzero positions of $\mathbf{x}_{|_t}$ consist only of elements of Lee weight 1. Therefore, it holds that $\mathrm{wt}_{\mathsf{L}}(\mathbf{x}_{|_t}) = \mathrm{wt}_{\mathsf{H}}(\mathbf{x}_{|_t}) \leq \mathrm{wt}_{\mathsf{L}}(\mathbf{c})$. Figure 7 gives empirical evidence supporting the result of Lemma V.1.

We can use these results to upper bound on the block error probability of a linear code over the memoryless Lee channel as a function of the codes Lee distance spectrum, for $\delta \leq \delta_q$.

**Corollary V.2.** *Consider an* $[n, k]$ *linear code* $\mathcal{C} \subset (\mathbb{Z}/q\mathbb{Z})^n$. *For all* $\ell \in \{0, \dots, n\lfloor q/2 \rfloor\}$ *let* $W_\ell^{(n)}(\mathcal{C})$ *denote the Lee weight enumerator of* $\mathcal{C}$. *The block error probability of* $\mathcal{C}$ *under ML decoding over the memoryless Lee channel* $\delta \leq \delta_q$ *is upper bounded as*

$$P_B(\mathcal{C}) \leq \sum_{\ell=1}^{n\lfloor q/2 \rfloor} W_\ell^{(n)}(\mathcal{C}) \mathbb{P}\left( \sum_{i=1}^{\min(\ell,n)} \Lambda_1 < 0 \right). \tag{22}$$

*Proof.* Recall from (20) that the block error probability of $\mathcal{C}$ is upper bounded by the sum of all pairwise error probabilities. By applying Lemma V.1 to the PEP-terms, the pairwise error probability can further be upper bounded by the probability of sending the zero codeword but decoding into a word whose nonzero elements are of Lee weight 1 only. □

**Example V.3.** Figure 8 depicts the union bound provided in Corollary V.2, together with the block error probability estimated via Monte Carlo simulation. For the comparison we used a linear code over $\mathbb{Z}/7\mathbb{Z}$ of length $n = 6$ and dimension $k = 2$ with generator matrix

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 3 & 3 & 3 & 0 \\ 0 & 1 & 0 & 4 & 3 & 3 \end{pmatrix}.$$

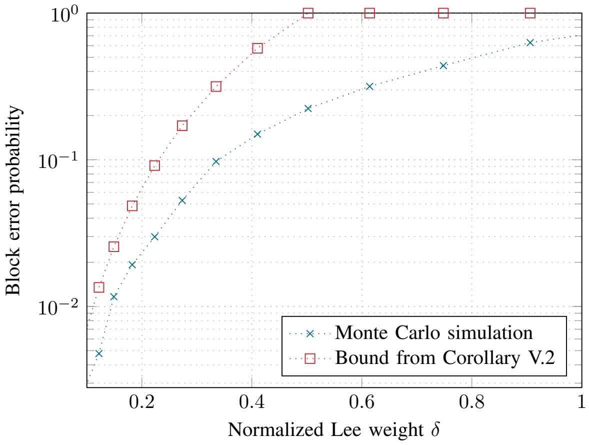

Fig. 8. Comparison of the union bound from Corollary V.2 with respect to the performance measured via Monte Carlo simulation for the linear code over $\mathbb{Z}/7\mathbb{Z}$ of length $n = 6$ and dimension $k = 2$ from Example V.3.

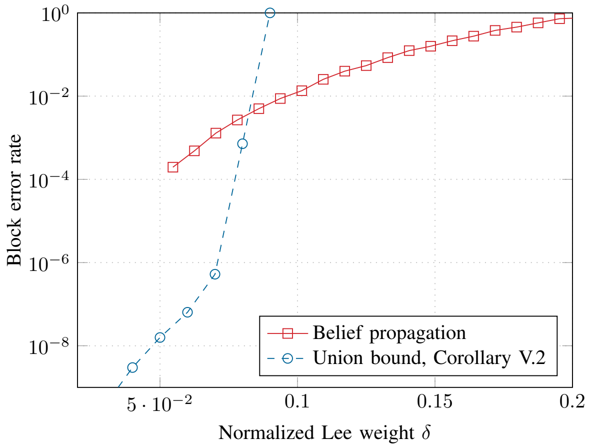

Fig. 9. Union bound versus belief propagation over $\mathbb{Z}/4\mathbb{Z}$ for a random $(3, 6)$ LDPC code of length $n = 256$.

As usually observed, the union bound provide accurate estimates at sufficiently low error probability.

The union bound of Corollary V.2 can be readily used to study the error floor performance of regular LDPC code ensembles. To do so, it is sufficient to replace the weight enumerator $W_\ell^{(n)}$ in (22) with the ensemble average enumerator $\overline{W}_\ell^{(n)}$. An example is provided in Figure 9, where the union bound on the ML decoding average block error probability for the $(3, 6)$-LDPC code ensemble of length $n = 256$ over $\mathbb{Z}/4\mathbb{Z}$ is depicted. The result is compared with the numerical simulation for a code from the ensemble, under BP decoding. As typical of union bounds on the block error probability, the bound is not informative above the cut-off rate of the channel. However, it provides an indication of the error probability regime at which an error floor may be observed, allowing for a quick estimation of the capability of certain code ensembles to attain given target error probabilities.

### B. Density Evolution Analysis

The analysis of the Lee spectrum of LDPC code ensembles can be used, in conjunction with the union bound, to analyze the ensembles behaviour under ML decoding at low error rates. Nevertheless, it fails to capture the block error probability behaviour in the waterfall region, under iterative decoding. We hence complement the distance spectrum analysis with a density evolution characterization of the ensemble in the limit of large block lengths. In particular, we estimate the asymptotic iterative decoding threshold over the memoryless Lee channel under BP and SMP decoding. The iterative decoding threshold $\delta^\star$ is defined as the largest value of the channel parameter $\delta$ for which, in the limit of large $n$ and large maximal number of iterations $\ell_{\max}$, the symbol error probability of an LDPC code picked randomly from a $(d_v, d_c)$ code ensemble becomes vanishing small [34]. Owing to the complexity of tracking the evolution of the distribution of multi-dimensional messages, under BP decoding we resort to the Monte Carlo method [35]. We denote by $\delta^\star_{\mathsf{BP}}$ the decoding threshold under BP decoding.

The density evolution analysis for the SMP decoder has been introduced in [21, Sec. IV]. We will briefly sketch the idea and emphasize the respective modifications according to the new memoryless Lee channel. For the SMP decoder the density evolution analysis not only aims at estimating the decoding threshold $\delta^\star_{\mathsf{SMP}}$ but it also provides bounds on the error probabilities $\xi$ of the extrinsic channel modelled as $q$-SC which are needed in the computation of the aggregated extrinsic log-likelihood vector (5). Since the memoryless Lee channel is symmetric and the code is linear, we can assume that the zero codeword has been transmitted. Similar to the notation used in the description of the SMP decoder, we let $m^{(\ell)}_{\mathsf{v}\to\mathsf{c}}$ denote the message sent from variable node $\mathsf{v}$ to check node $\mathsf{c}$ in the $\ell$-th iteration. For every $a \in \mathbb{Z}/q\mathbb{Z}$, let us define the probability of sending a message $m^{(\ell)}_{\mathsf{v}\to\mathsf{c}} = a$, knowing that originally zero has been transmitted as

$$p^{(\ell)}_a := \mathbb{P}\left(m^{(\ell)}_{\mathsf{v}\to\mathsf{c}} = a \,|\, X = 0\right).$$

Hence, recalling the memoryless Lee channel transition probability $P_{Y\,|\,X}(y\,|\,x)$ from (6), we initialize the density evolution analysis by computing for each $a \in \mathbb{Z}/q\mathbb{Z}$ the probabilities

$$p^{(0)}_a = P_{Y\,|\,X}(a\,|\,0).$$

As indicated above, except from the computation of the aggregated extrinsic likelihood vector, the remaining steps of the density evolution analysis are identical to [21, Sec. IV]. In particular, we employ the $q$-SC approximation for the extrinsic channel.

Table I records the decoding thresholds $\delta^\star_{\mathsf{SMP}}$ and $\delta^\star_{\mathsf{BP}}$ for the SMP and BP decoder, respectively, for both $(3,6)$ and $(4,8)$ regular LDPC code ensembles with $q$ ranging from 5 to 8, as well as the Shannon limit $\delta^\star_{\mathsf{SH}}$ which is given by the solution in $\delta$ of $R_2 = \log_2(q) - H(B_\delta)$ for the rate $R_2 = 1/2$.

TABLE I
DECODING THRESHOLDS FOR REGULAR LDPC CODE ENSEMBLES UNDER BP AND SMP DECODING.

| $q$ | $(v,c)$ | $\delta^\star_{\mathsf{BP}}$ | $\delta^\star_{\mathsf{SMP}}$ | $\delta^\star_{\mathsf{SH}}$ |
|---|---|---|---|---|
| 5 | $(3,6)$ | 0.2148 | 0.1039 | 0.2684 |
| | $(4,8)$ | 0.1802 | 0.1200 | |
| 6 | $(3,6)$ | 0.2485 | 0.1151 | 0.3147 |
| | $(4,8)$ | 0.2217 | 0.1405 | |
| 7 | $(3,6)$ | 0.3086 | 0.1261 | 0.3560 |
| | $(4,8)$ | 0.2686 | 0.1539 | |
| 8 | $(3,6)$ | 0.3135 | 0.1374 | 0.3950 |
| | $(4,8)$ | 0.26904 | 0.1623 | |

**Remark V.4.** The choice of the DMC used to model the extrinsic channel plays a crucial role for the SMP algorithm, especially concerning the decoding performance. In [27], for the case of BMP decoding, it was suggested to model the VN inbound messages as observations of a binary symmetric channel (BSC), whose transition probability was estimated by means of density evolution analysis. The approach was generalized in [21] for SMP, where the VN inbound messages are modelled as observations of a $q$-SC. In our setting we will also model the extrinsic channel as a $q$-SC defined in (4), although in our setting the $q$-SC model holds only in an approximate sense.

The adoption of the $q$-SC approximation is particularly useful from a practical viewpoint since the VN processing in SMP decoding becomes particularly simple if the VN-to-CN messages are assumed to be observations of an extrinsic $q$-SC. Moreover, this specific choice is motivated by the fact that, for LDPC codes over finite fields, the extrinsic channel transition probabilities, averaged over a uniform distribution of nonzero elements in the parity-check matrix, yield (in the limit of a large block length) a $q$-SC [21]. The following Lemma for $q$ prime, whose proof is trivial, supports this statement.

**Lemma V.5.** *Consider a prime number $q$. Let $H$ be a random variable drawn uniformly at random form the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^\times$ and let $X$ be any random variable over $\mathbb{Z}/q\mathbb{Z}$. Define the random variable $V = X \cdot H$. Then $V$ follows a $q$-SC-like distribution given as*

$$\mathbb{P}(V = v) = \begin{cases} \mathbb{P}(X = 0) & \textit{if } v = 0 \\ \frac{1}{q-1}(1 - \mathbb{P}(X = 0)) & \textit{else.} \end{cases}$$

Even though for $q$ is non-prime the average extrinsic channel transition probabilities can not be represented by a $q$-SC, we still make this assumption. The Empirical evidence obtained by measuring the total variation distance between the true extrinsic channel and the $q$-SC shows that the $q$-SC can still be used to accurately model the actual extrinsic channel, especially if the ring possesses relatively many unit elements. More precisely, we show numerically that the total variation distance between the two message distributions tends to zero as the number of iteration grows. We denote by $\mathcal{U}_q$ the fraction of units in $\mathbb{Z}/q\mathbb{Z}$, i.e.,

$$\mathcal{U}_q := \frac{|(\mathbb{Z}/q\mathbb{Z})^\times|}{|\mathbb{Z}/q\mathbb{Z}|}.$$

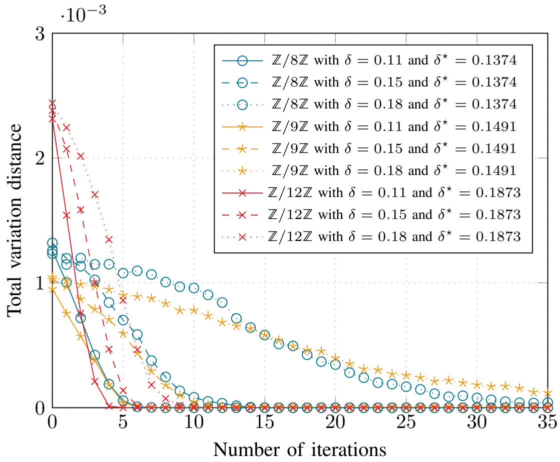

Fig. 10. Evolution of the TV distance between the extrinsic channel distribution and the $q$-SC for regular $(3, 6)$ LDPC code ensembles in the SMP decoder.

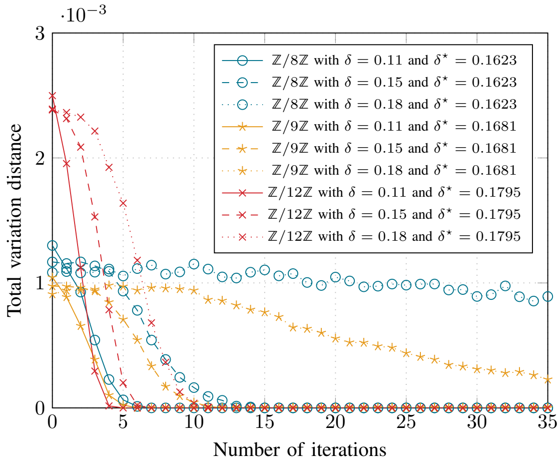

Fig. 11. Evolution of the TV distance between the extrinsic channel distribution and the $q$-SC for regular $(4, 8)$ LDPC code ensembles in the SMP decoder.

In order to cover different cases and support the conjecture that the $q$-SC assumption is especially accurate for integer rings with relatively many units, we chose three integer rings having different fractions of units. Namely, we chose $\mathbb{Z}/8\mathbb{Z}$ with $\mathcal{U}_8 = 1/2$, $\mathbb{Z}/9\mathbb{Z}$ with $\mathcal{U}_9 = 2/3$ and $\mathbb{Z}/12\mathbb{Z}$ with $\mathcal{U}_{12} = 1/3$. Figures 10, 11 and 12 show the evolution of the total variation distance with the number of iterations for different regular LDPC code ensembles, respectively. In each figure and for each integer ring, we consider three different situations: one where the relative Lee weight $\delta$ is below $\delta^\star_{\mathsf{SMP}}$, one where $\delta$ is close to $\delta^\star_{\mathsf{SMP}}$ and one where the relative Lee weight exceeds the threshold. The figures clearly support the conjecture on the fraction of units $\mathcal{U}_q$ as well as the choice to model the average extrinsic channel transition probabilities by a $q$-SC.

### C. Numerical Results

We finally present numerical results showing the decoding performance (in terms of block error rates) of $(3, 6)$ regular LDPC codes of length $n = 256$ under both BP and SMP decoding. We chose to analyze the performances over three different integer rings, namely $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$ and $\mathbb{Z}/8\mathbb{Z}$. The performances will additionally be compared to the LSF decoder presented in [22, Algorithm 2]. Following the suggestions of [22], we assumed a decoding threshold $\tau = \frac{d_\mathsf{v}}{2}$ for the LSF decoder. All the results were obtained using Monte Carlo simulations. The codes used in the simulations have been obtained by first generating their bipartite graphs via the progressive edge growth (PEG) algorithm [36], and then by assigning to the nonzero entries in the code parity-check matrices elements sampled uniformly at random and independently from $(\mathbb{Z}/q\mathbb{Z})^\times$. The error vectors in the constant Lee weight channel are drawn uniformly at random from the Lee sphere of a given radius representing the desired weight according to [8, Algorithms 1 and 2], whereas in the memoryless Lee channel the entries of the error vector are drawn according to the distribution defined in (6). In both cases, the performance is compared to the RCU bounds established in Corollary III.4 and Theorem III.7, respectively.

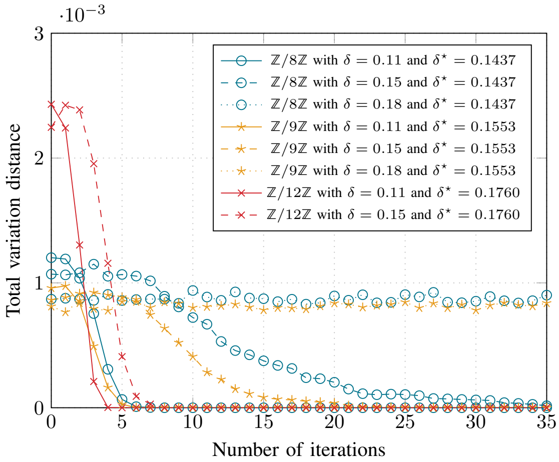

Fig. 12. Evolution of the TV distance between the extrinsic channel distribution and the $q$-SC for regular $(5, 10)$ LDPC code ensembles in the SMP decoder.

The block error probability evaluated over the memoryless channel is shown in Figure 13. The RCU bounds (dotted in the graph) show clearly the impact of the size $q$ of the finite integer ring, i.e., larger $q$ admit a larger relative Lee weight $\delta$. This is also observed in the performance under both BP and SMP decoding as well as in the LSF decoder. The impact of $q$ in the SMP is not only important for the admissible choices of $\delta$. Moreover it shows clearly the difference between $q$ prime and not. While a small gain is achieved when considering $\mathbb{Z}/8\mathbb{Z}$ instead of $\mathbb{Z}/7\mathbb{Z}$ under BP decoding, the performance slightly suffers under SMP decoding meaning there is almost no gain. This might be due to the $q$-SC assumption which holds only in an asymptotic sense for the non-field case, as discussed in Section V-B.

We observe the same effect in the performance over the constant Lee weight channel in Figure 14, i.e. there is almost no gain visible when moving from $q = 7$ to $q = 8$ under the SMP decoder. Analogous to the memoryless case, we observe the same impact of the size of $\mathbb{Z}/q\mathbb{Z}$ on the possible choices

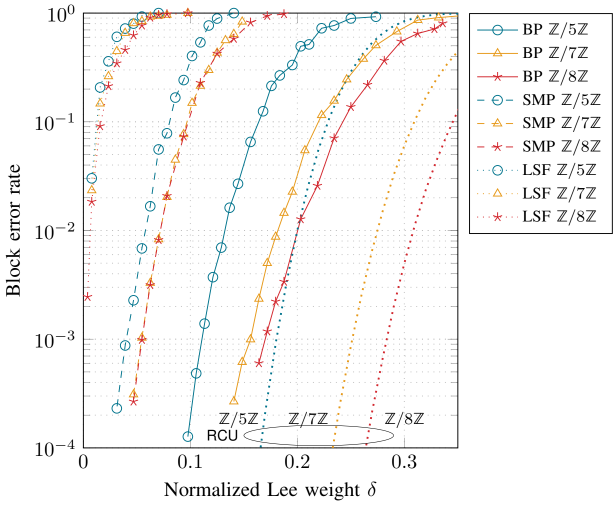

Fig. 13. Block error rate vs. $\delta$ for regular $(3, 6)$ nonbinary LDPC codes of length $n = 256$, memoryless Lee channel. LSF compared to the RCU bound from Theorem III.7, SMP and BP decoding.

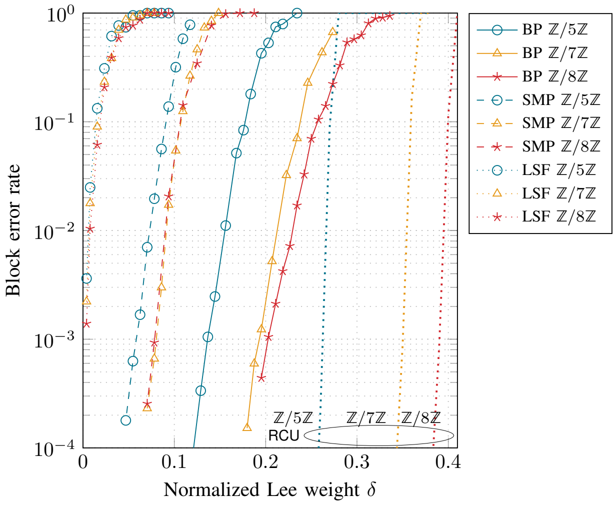

Fig. 14. Block error rate vs. $\delta$ for regular $(3, 6)$ nonbinary LDPC code ensembles of length $n = 256$ and rate $R = 1/2$ on the constant Lee weight channel under LSF, SMP and BP decoding compared to the RCU bound from Theorem III.3.

of $\delta$ which is captured by the RCU bound for the constant Lee weight channel. In both channel models we observe that the SMP decoder outperforms the LSF decoder despite the $q$-SC assumption in the extrinsic channel of the SMP. We want to emphasize and acknowledge here that the LSF was originally designed for low-Lee-density parity-check codes which form a special class of LDPC codes. Hence, when comparing the performances over the two decoders the difference of the code classes might be taken in consideration. Nevertheless, we will not focus deeper on this argument and leave this subject to future investigations. We believe that the additional knowledge about the marginal distribution plays a crucial part in the performance gain under SMP decoding. Observe that the estimated threshold values obtained via density evolution analysis and stored in Table I match well to the actual block error rates achieved by both BP and SMP decoding. As expected from the predictions in Table I, BP clearly outperforms SMP decoding. However, the SMP algorithm shows a performance that is appealing for applications demanding low-complexity decoding [22].

## VI. Conclusions

In this paper we studied the decoding performance of random regular low-density parity-check (LDPC) codes over finite integer rings considering two channel models in the Lee metric, a memoryless channel model and a channel introducing an error of given Lee weight. We established the growth rate spectra of the Lee sphere and Lee volume, respectively. These results were used to derive random coding union bounds for the block error probability under maximum likelihood and minimum distance decoding for both channel models. In the case of the memoryless Lee channel we also derived a lower bound (in terms of a sphere packing bound) on the error probability. An upper bound on the ML block error probability of linear codes based on the Lee weight enumerator of the code was introduced. The bound has been used to study the average block error probability of regular LDPC code ensembles, thanks to a derivation of the average Lee weight spectrum of the ensembles. The bound provides relevant information on the code performance in the low error probability regime (i.e., in the error floor region). The study has been complemented with a density evolution analysis. Two decoders have been considered: one based on the (non-binary) belief propagation algorithm, and a low-complexity message-passing algorithm where exchanged messages are hard symbols (i.e., ring elements). The simulation results confirmed the outcomes of the density evolution analysis, that is belief propagation decoding outperforms symbol message passing decoding. Nevertheless, the performance under symbol message passing decoding seems a promising option for applications asking for low complexity (such as code-based cryptosystems involving the Lee metric). Furthermore, the performance analysis of regular LDPC codes over integer residue rings that we developed might be useful to design such LDPC codes for applications to cryptography.

In this work, we restricted ourselves to regular LDPC codes over integer residue rings. Future work includes the performance study of other families of LDPC codes over finite integer rings such as protograph-based and irregular LDPC codes.

## References

[1] C. Lee, “Some properties of nonbinary error-correcting codes,” *IRE Trans. Inf. Theory*, vol. 4, no. 2, pp. 77–82, 1958.
[2] W. Ulrich, “Non-binary error correction codes,” *The Bell System Technical Journal*, vol. 36, no. 6, pp. 1341–1388, 1957.
[3] E. R. Berlekamp, “Negacyclic codes for the Lee metric,” North Carolina State University. Dept. of Statistics, Tech. Rep., 1966.
[4] J. C.-Y. Chiang and J. K. Wolf, “On channels and codes for the Lee metric,” *Information and Control*, vol. 19, no. 2, pp. 159–173, 1971.
[5] T. Etzion, A. Vardy, and E. Yaakobi, “Dense error-correcting codes in the Lee metric,” in *Proc. IEEE Information Theory Workshop*, Sep. 2010.
[6] S. W. Golomb and L. R. Welch, “Algebraic coding and the Lee metric,” *Error Correcting Codes*, pp. 175–194, 1968.
[7] E. Prange, “The use of coset equivalene in the analysis and decoding of group codes,” Air Force Cambridge Research Labs, Tech. Rep., 1959.

[8] J. Bariffi, H. Bartz, G. Liva, and J. Rosenthal, “On the properties of error patterns in the constant Lee weight channel,” in *Proc. International Zurich Seminar on Information and Communication (IZS)*, Zurich, Switzerland, Mar. 2022, pp. 44–48.

[9] J. Bariffi, K. Khathuria, and V. Weger, “Information set decoding for Lee-metric codes using restricted balls,” in *Proc. Code-Based Cryptography: 10th International Workshop, CBCrypto 2022 - Revised Selected Papers*. Lecture Notes in Computer Science, Springer, 2023.

[10] A. Chailloux, T. Debris-Alazard, and S. Etinski, “Classical and quantum algorithms for generic syndrome decoding problems and applications to the Lee metric,” in *Proc. International Conference on Post-Quantum Cryptography*. Springer, 2021, pp. 44–62.

[11] S. Ritterhoff, G. Maringer, S. Bitzer, V. Weger, P. Karl, T. Schamberger, J. Schupp, and A. Wachter-Zeh, “FuLeeca: A Lee-based Signature Scheme,” Cryptology ePrint Archive, Paper 2023/377, 2023. [Online]. Available: https://eprint.iacr.org/2023/377

[12] V. Weger, K. Khathuria, A.-L. Horlemann, M. Battaglioni, P. Santini, and E. Persichetti, “On the hardness of the Lee syndrome decoding problem,” *Advances in Mathematics of Communications*, vol. 18, no. 1, pp. 233–266, 2024.

[13] R. M. Roth and P. H. Siegel, “Lee-metric BCH codes and their application to constrained and partial-response channels,” *IEEE Trans. Inf. Theory*, vol. 40, no. 4, pp. 1083–1096, Apr. 1994.

[14] R. Gabrys, H. M. Kiah, and O. Milenkovic, “Asymmetric Lee distance codes for DNA-based storage,” *IEEE Trans. Inf. Theory*, vol. 63, no. 8, pp. 4982–4995, Aug. 2017.

[15] J. Astola, “On the asymptotic behaviour of Lee-codes,” *Discrete Applied Mathematics*, vol. 8, no. 1, pp. 13–23, 1984.

[16] E. Byrne and V. Weger, “Bounds in the lee metric and optimal codes,” *Finite Fields and Their Applications*, vol. 87, p. 32, 2023.

[17] H.-A. Loeliger, “An upper bound on the volume of discrete spheres,” *IEEE Trans. Inf. Theory*, vol. 40, no. 6, pp. 2071–2073, 1994.

[18] R. Gallager, “Low-density parity-check codes,” *IRE Trans. Inf. Theory*, vol. 8, no. 1, pp. 21–28, 1962.

[19] D. Sridhara and T. E. Fuja, “LDPC codes over rings for PSK modulation,” *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3209–3220, Sep. 2005.

[20] M. Davey and D. MacKay, “Low density parity check codes over GF($q$),” *IEEE Commun. Lett.*, vol. 2, no. 6, pp. 70–71, Jun. 1998.

[21] F. Lazaro, A. Graell i Amat, G. Liva, and B. Matuz, “Symbol message passing decoding of nonbinary low-density parity-check codes,” in *Proc. IEEE Global Communications Conference*, Dec. 2019.

[22] P. Santini, M. Battaglioni, F. Chiaraluce, M. Baldi, and E. Persichetti, “Low-Lee-density parity-check codes,” in *Proc. IEEE International Conference on Communications (ICC)*, Jun. 2020.

[23] A. D. Wyner and R. L. Graham, “An upper bound on minimum distance for a $k$-ary code,” *Information and Control*, vol. 13, no. 1, pp. 46–52, 1968.

[24] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. New York: Wiley, 2006.

[25] L. Boltzmann, “Studien über das Gleichgewicht der lebendigen Kraft zwischen bewegten materiellen Punkten (Studies of the equilibrium and the life force between material points),” *Wien. Ber*, vol. 58, p. 517, 1868.

[26] E. L. Wilmer, D. A. Levin, and Y. Peres, “Markov chains and mixing times,” *American Mathematical Soc., Providence*, 2009.

[27] 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, 2011.

[28] 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, Nov. 2004.

[29] R. Gallager, *Information theory and reliable communication*. New York, NY, USA: Wiley, 1968.

[30] L. C. Grove, *Algebra*. Academic Press, 1983.

[31] W. K. Hayman, “A generalisation of Stirling’s formula.” *Journal für die reine und angewandte Mathematik*, vol. 196, pp. 67–95, 1956.

[32] H. S. Wilf, *Generatingfunctionology*. CRC press, 2005.

[33] C. Di, “Asymptotic and finite-length analysis of low-density parity-check codes,” Ph.D. dissertation, Ecole Polytechnique Fédérale de Lausanne, Lausanne, Switzerland, 2004.

[34] T. Richardson and R. Urbanke, “The capacity of low-density parity-check codes under message-passing decoding,” *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 599–618, Feb. 2001.

[35] M. C. Davey and D. J. MacKay, “Monte Carlo simulations of infinite low density parity check codes over GF(q),” in *Proc. Int. Workshop on Optimal Codes and Related Topics*, Bulgaria, Jun. 1998, pp. 9–15.

[36] X.-Y. Hu, E. Eleftheriou, and D. Arnold, “Regular and irregular progressive edge-growth Tanner graphs,” *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 386–398, Jan. 2005.

**Jessica Bariffi** (IEEE Student Member) was born in Zurich, Switzerland in 1995. She received her M.Sc. and Ph.D. degrees in mathematics from the University of Zurich, Switzerland, in 2020 and 2024, respectively. In her dissertation (supervised by Prof. Joachim Rosenthal) she studied the algebraic structure of Lee-metric codes, the decoding performance of LDPC codes over suitably designed channels in the Lee metric, as well as Information Set Decoding in the Lee metric. She pursued her Ph.D. together with the German Aerospace Center (DLR) in Munich, Germany, where she worked in the Quantum-Resistant Cryptography group under Dr. Hannes Bartz. In July 2024 she started a postdoc position at the Technical University of Munich, Germany, at the Institute for Communications Engineering under the supervision of Prof. Antonia Wachter-Zeh.

**Hannes Bartz** (S’14-M’16) was born in Trostberg, Germany, in 1985. He received his Dipl.-Ing. and Dr.-Ing. degree from the Technical University of Munich, Germany, in 2010 and 2017, respectively. In his dissertation (supervised by Prof. Gerhard Kramer) he developed efficient algebraic decoding schemes for error-correcting codes in subspace and rank metric. In July 2017 he joined the Information Transmission Group within the Institute of Communications and Navigation at the German Aerospace Center (DLR). Since April 2021 he is leading the Quantum-Resistant Cryptography (QRC) group within the Satellite Networks department. His main research interests are code-based post-quantum cryptography and algebraic coding theory. In 2018 he has been appointed as a Lecturer at the Institute for Communications Engineering (LNT), Technical University of Munich, Germany. He received the Prof. Dr. Ralf Kötter memorial award in 2012.

**Gianluigi Liva** (M’08–SM’14) was born in Spilimbergo, Italy, in 1977. He received the M.S. and Ph.D. degrees in electrical engineering from the University of Bologna, Italy, in 2002 and 2006, respectively. Since 2003 he has been investigating channel codes for high-data rate Consultative Committee for Space Data Systems (CCSDS) missions. From 2004 to 2005, he was involved in research at the University of Arizona, Tucson. Since 2006, he has been with the Institute of Communications and Navigation, German Aerospace Center (DLR), where he currently leads the Information Transmission Group. In 2010, he has been appointed as a Lecturer of channel coding with the Institute for Communications Engineering (LNT), Technical University of Munich (TUM). From 2012 to 2013, he was a Lecturer of channel coding with the Nanjing University of Science and Technology, China. Since 2014, he has been a Lecturer of channel codes with iterative decoding with LNT, TUM. He received the Italian National Scientific Habilitation (ASN) as Full Professor in Telecommunication Engineering in July 2017. His main research interests include satellite communications, random access techniques, and error control coding. He is/has been active in the DVB-SH, DVB-RCS, and DVB-S2 standardization groups, and in the standardization of error correcting codes for deep-space communications within the CCSDS. He was the co-chair of the 2018 IEEE European School on Information Theory, the sponsor co-chair of the IEEE Information Theory Workshop 2020 in Riva del Garda, and the TPC co-chair of the 2023 International Symposium on Topics in Coding. Since 2020, he serves as Associate Editor in Coding and Information Theory for the IEEE Transactions on Communications.

**Joachim Rosenthal** (Fellow, IEEE) received the Diploma degree in mathematics from the University of Basel in 1986 and the Ph.D. degree in mathematics from Arizona State University in 1990. From 1990 to 2006, he was with the University of Notre Dame, USA, where he was the holder of an Endowed Chair of applied mathematics and he was also a Concurrent Professor of electrical engineering. Since 2004, he has been a Professor of applied mathematics with the University of Zurich, where was the past Chair of the Institute of Mathematics and the Vice Dean of the College of Science. He will be (2024–2025) the President of the Swiss Mathematical Society. His current research interests include coding theory and cryptography. He has served as an organizer or the program chair for numerous international conferences, e.g., he is one of the Technical Program Chair of ISIT 2024, Athens, Greece. In addition, he has served on numerous editorial boards.