LDPC Codes over the q-ary Multi-Bit Channel

Rami Cohen, *Graduate Student Member, IEEE,* Netanel Raviv, *Member, IEEE,* and Yuval Cassuto, *Senior Member, IEEE*

Abstract**—In this paper, we introduce a new channel model we term the q-ary multi-bit channel (QMBC). This channel models a memory device, where q-ary symbols ($q = 2^s$) are stored in the form of current/voltage levels. The symbols are read in a measurement process, which provides a symbol bit in each measurement step, starting from the most significant bit. An error event occurs when not all the symbol bits are known. To deal with such error events, we use GF(q) low-density parity-check (LDPC) codes and analyze their decoding performance. We start with iterative-decoding threshold analysis, and derive optimal edge-label distributions for maximizing the decoding threshold. We later move to finite-length iterative-decoding analysis and propose an edge-labeling algorithm for improved decoding performance. We then provide finite-length maximum-likelihood decoding analysis for both the standard non-binary random ensemble and LDPC ensembles. Finally, we demonstrate by simulations that the proposed edge-labeling algorithm improves finite-length decoding performance by orders of magnitude.**

I. Introduction

In multi-level memories, information is often stored in the form of $q = 2^s$ (for some integer s) voltage/current levels. In the read process, the stored levels are measured and converted to a q-ary symbol. In this work, we introduce the *q-ary multi-bit channel* (QMBC) model for imperfectly reading information from memory devices. The QMBC is a special case of a *partial-erasure channel* [1], where the channel output is a *set* containing the input symbol.

In the QMBC, each q-ary symbol is decomposed into s bits with hierarchical structure. The bits are organized such that when the channel erases bit $j \in \{1,\dots,s\}$, all lower bits $\{1,\dots,j-1\}$ are erased as well. That is, the QMBC directly models a readout by a binary-search sequence that may terminate while the last j measurements are missing. The channel outputs in the QMBC are either the input symbol, or a set of 2^j ($j \in \{1,...,s\}$) *consecutive* symbols that contain the input symbol. In the latter case, we say that a *partial-erasure* event occurred. For example, in the highest-severity partial-erasure event that is not a full erasure, the output set contains either the lower or upper $q/2$ symbols. This model is different from the q-ary partial-erasure channel (QPEC) model [1], where the channel output is a random set containing the input symbol.

The hierarchical structure of the QMBC puts it in lineage with prior coding schemes that exhibit hierarchy among bits in the code symbol. For example, a partition rule based on the significance of the bits is proposed in the seminal paper of Ungerboeck [2]. In [3], a wireless-network receiver observes only the upper bits of the transmitted symbols, where the number of bits depends on the channel gain. Hence this paper's theoretical framework for designing LDPC codes for the QMBC may find use in applications other than the specific one mentioned above in non-volatile memories. Our choice to define the QMBC as an erasure-type channel is made for the sake of mathematical preciseness and theoretical insight, which are much harder to obtain with error-type channels. That said, classical LDPC theory has shown that binary erasures are a good proxy for symmetric bit errors, and we believe that QMBC partial erasures are a similarly good proxy for natural errors in non-volatile memories, such as graded-magnitude errors [4].

To deal with QMBC partial-erasure events, we use GF(q) low-density parity-check (LDPC) codes [5], [6], due to their good performance under iterative decoding. We show that messages exchanged in the iterative-decoding process have certain structural properties that facilitate decoding-performance analysis. To obtain a suitable measure of asymptotic iterative-decoding performance, we extend the binary erasure channel (BEC) decoding threshold [7], by defining the QMBC *decoding threshold region*. We use the structure of the messages to both simplify the decoding-threshold region analysis and to derive an optimal code-graph edge label distribution for maximal performance.

We later move to design and analysis of *finite-length* LDPC codes for the QMBC. When iterative decoding is applied over the QMBC, in addition to the stopping sets [8], the finite-length performance depends strongly on the edge labels. We theoretically characterize this dependence by analyzing the algebraic structure of the partial-erasure sets within the finite field, and propose an edge-labeling algorithm that considerably mitigates the harmful effect of stopping sets. In that, our work extends previous label-optimization algorithms (e.g., [9], [10]) to the special structure of the QMBC. The advantage here is that the QMBC has strong solvability conditions that are local to a single check, and thus allow neutralizing stopping sets even without relying on the cycle structure of the graph. We demonstrate the use of *universal* edge labels for local solvability at the check node for all combinations of two QMBC partial-erasure sizes that satisfy $j_1 + j_2 \leq s$. We then study the QMBC finite-length maximum-likelihood decoding performance, both for the standard non-binary ensemble and

The first and third authors are with the Andrew and Erna Viterbi Faculty of Electrical Engineering, Technion - Israel Institute of Technology, Haifa, Israel 3200003 (email: rc@technion.ac.il, ycassuto@ee.technion.ac.il); the second author is with the Department of Electrical Engineering, California Institute of Technology, Pasadena 91125, CA, USA (email: netanel.raviv@gmail.com). The work is supported in part by the Israel Science Foundation, by the US-Israel Binational Science Foundation, and by the Henri Gutwirth Fund for Promotion of Research.

Parts of this work were presented at the 9th International Symposium on Turbo Codes & Iterative Information Processing (ISTC), September 2016, Brest, France and at the 2017 IEEE International Symposium on Information Theory (ISIT), June 2017, Aachen, Germany.

regular LDPC ensembles. Because QMBC erasures are *subsets* of the field GF(q), the main analytical challenge here is in losing the linear structure. Finally, simulation results show that our edge-labeling algorithm offers significant improvement over uniform labeling, and even more so compared to using a binary LDPC code.

This paper is structured as follows. In Section II, the QMBC model and an iterative message-passing decoder are provided. Structural properties of the iterative decoder are given in Section III. The QMBC decoding-threshold region and optimal edge-label distributions are introduced in Section IV. Finite-length analysis of iterative-decoding performance and an edge-labeling algorithm for improved decoding performance are presented in Section V. We study finite-length *maximum-likelihood* decoding performance in Section VI. Finally, simulation results are presented in Section VII and conclusions are provided in Section VIII.

II. Channel Model and Iterative Decoder

The q-ary multi-bit channel (QMBC) belongs to the class of partial-erasure channels [1], where the read process provides either the correct symbol or a *partially-erased* symbol. In the latter case, a subset of the input symbols that contains the correct symbol is provided as the channel output. The binary and the q-ary erasure channels (BEC and QEC) are special cases of the QMBC, where *full* erasures may occur, carrying no non-trivial information.

A. Channel model and capacity

The QMBC input alphabet consists of $q = 2^s$ symbols: $\mathcal{X} = \{0, 1, ..., q-1\}$, for some integer s. For each input symbol x and $j = 0, 1, 2, ..., s$, a *partial-erasure* event of type j occurs when only the $s-j$ left bits of x in binary representation are known. In this case, the channel output is a set of 2^j consecutive symbols that have the same $s-j$ left bits as x. We denote this output set by $\mathcal{M}_x^j$. Note that $x \in \mathcal{M}_x^j$ for any j, i.e., the correct input symbol belongs to the output set. In addition, the input symbol is completely known when $j = 0$. The transition probabilities governing the QMBC are:

$$\Pr\left(Y = \mathcal{M}_x^j \middle| X = x\right) = \varepsilon_j, \tag{1}$$

where ε_j for $j = 0, 1, ..., s$ are the partial-erasure probabilities. Note that for $\varepsilon_1 = \varepsilon_2 = ... = \varepsilon_{s-1} = 0$ the QMBC reduces to the QEC, and when $s = 1$ the QMBC reduces to the BEC.

Example 1. *Assume that* $q = 4$. *Then* $\mathcal{M}_0^1 = \mathcal{M}_1^1 = \{0, 1\}, \mathcal{M}_2^1 = \mathcal{M}_3^1 = \{2, 3\}, \mathcal{M}_0^2 = \mathcal{M}_1^2 = \mathcal{M}_2^2 = \mathcal{M}_3^2 = \{0, 1, 2, 3\}$.

We now move to provide the QMBC capacity.

Theorem 1. *The QMBC capacity is*

$$1 - \sum_{j=1}^{s} \frac{j\varepsilon_j}{s}, \tag{2}$$

measured in q-ary symbols per channel use.

The proof is similar to the proof of [1, Theorem 1] and is omitted. The QMBC capacity (2) implies that a QMBC has the same capacity as a BEC with erasure probability $\sum_{j=1}^{s} j\varepsilon_j/s$. Note that if the only non-zero partial-erasure probability is ε_s, the QMBC capacity reduces to the QEC capacity $1 - \varepsilon_s$, as expected.

B. GF(q) representation

For analysis purposes, we map the symbols in $\mathcal{X}$ to GF($q = 2^s$) elements. Consider a basis $\{\omega_1, \omega_2, ..., \omega_s\}$ of GF($q = 2^s$) over GF(2). Denote by $\langle\omega_1, \omega_2, ..., \omega_j\rangle$ the span of the basis elements $\omega_1, \omega_2, ..., \omega_j$ for $j = 1, 2, ..., s$. As an example, $\langle\omega_1, \omega_2\rangle = \{a \cdot \omega_1 + b \cdot \omega_2 : a, b \in \{0, 1\}\}$. We map the sets $\mathcal{M}_0^j$ for $j = 1, 2, ..., s$ to $\langle\omega_1, \omega_2, ..., \omega_j\rangle$, which are *subgroups* of the additive group of GF(q). These subgroups are linear subspaces of the field GF($q = 2^s$) when viewed as a dimension-s vector space over GF(2). More generally, for each $j = 1, 2, ..., s$ and $x \in \mathcal{X}$ we map $\mathcal{M}_x^j$ to the 2^{s-j} cosets of $\langle\omega_1, \omega_2, ..., \omega_j\rangle$, where the coset representatives are taken from $\langle\omega_{j+1}, \omega_{j+2}, ..., \omega_s\rangle$.

Example 2. Let α designate a root of the primitive polynomial $x^2 + x + 1$ such that $\{1, \alpha\}$ is a basis of GF(4) over GF(2). The sets $\mathcal{M}_0^0, \mathcal{M}_0^1$ and $\mathcal{M}_0^2$ are mapped to the subgroups $\{0\}, \{0, 1\}$ and $\{0, 1, \alpha, \alpha+1\}$, respectively. The cosets of $\{0, 1\}$ are $\{0, 1\}$ and $\{\alpha, \alpha+1\}$. Thus, $\mathcal{M}_1^1$ is mapped to $\{0, 1\}$, while $\mathcal{M}_2^1$ and $\mathcal{M}_3^1$ are mapped to $\{\alpha, \alpha+1\}$.

We will assume a mapping as above, and will refer to symbol/field representation of the elements in $\mathcal{X}$ interchangeably.

C. GF(q) LDPC codes

The error-correcting codes we consider for dealing with the QMBC are GF(q) LDPC codes [5], [6]. These codes are defined by a sparse parity-check matrix with elements taken from GF(q). This matrix is commonly visualized as a Tanner graph [11]. The graph is bipartite, with *variable* (left) nodes corresponding to codeword symbols, and *check* (right) nodes corresponding to parity-check equations. The edge labels on the graph are taken from the non-zero elements of GF(q). The parity-check equation induced by check node c is $\sum_{\mathsf{v} \in \mathcal{N}(\mathsf{c})} h_{\mathsf{c},\mathsf{v}} \cdot \mathsf{v} = 0$, where $\mathcal{N}(\mathsf{c})$ is the set of variable nodes adjacent to check node c and $h_{\mathsf{c},\mathsf{v}}$ is the label on the edge connecting check node c to its neighbour $\mathsf{v} \in \mathcal{N}(\mathsf{c})$. The calculations are performed using the GF(q) arithmetic.

LDPC codes are usually characterized by the *degree distributions* of the variable and check nodes. They are called *regular* if both variable nodes and check nodes have constant degree. Otherwise, they are called *irregular*. Denote by d_v and d_c the maximal degree of variable nodes and check nodes, respectively. As is customary [7], we define the degree-distribution polynomials $\lambda(x) = \sum_{i=2}^{d_v} \lambda_i x^{i-1}$ and $\rho(x) = \sum_{i=2}^{d_c} \rho_i x^{i-1}$, where a fraction λ_i (ρ_i) of the edges is connected to variable (check) nodes of degree i. The *design* *rate* R of an LDPC code, measured in q-ary symbols per channel use, is [7]:

$$R = 1 - \left(\sum_{i=2}^{d_c} \rho_i/i\right) / \left(\sum_{i=2}^{d_v} \lambda_i/i\right). \tag{3}$$

The design rate equals the actual rate if the rows of the LDPC code parity-check matrix are linearly independent. Otherwise, the design rate is a lower bound on the actual rate.

D. Set iterative decoder

Since the QMBC belongs to the class of partial-erasure channels, we use the iterative decoder suggested for such channels in [1]. In this decoder, sets of symbols are exchanged as messages in the decoding process. The set iterative decoder extends the BEC iterative decoder [7] to partial erasures, as follows. As usual, we have *variable-to-check* (VTC) and *check-to-variable* (CTV) messages. We denote by $\mathrm{CTV}_{\mathtt{c}\to\mathtt{v}}^{(l)}$ the CTV message from check node $\mathtt{c}$ to variable node $\mathtt{v}$ at iteration l. In a similar way, $\mathrm{VTC}_{\mathtt{v}\to\mathtt{c}}^{(l)}$ denotes the VTC message at iteration l. Both the VTC and CTV messages are *sets* containing GF(q) elements.

An outgoing message from a graph node to a target (adjacent) node depends on incoming messages along edges connected to the source node except the outgoing message edge. At iteration $l = 0$ (initialization), variable node $\mathtt{v}$ sends its channel-information set (which can be one of the sets $\mathcal{M}_x^j$ defined in Section II-A) to adjacent check nodes. We denote these initial messages by $\mathrm{VTC}_{\mathtt{v}}^{(0)}$.

A CTV message $\mathrm{CTV}_{\mathtt{c}\to\mathtt{v}}^{(l)}$ contains all the possible symbol values of $\mathtt{v}$ that satisfy the parity-check equation at $\mathtt{c}$ given the VTC messages to $\mathtt{c}$ at iteration $l-1$. To calculate the CTV messages efficiently, the *sumset* operation [12] is used. This operation is defined for two sets $\mathcal{A}$ and $\mathcal{B}$ that contain GF(q) elements as

$$\mathcal{A} + \mathcal{B} \triangleq \{a + b : a \in \mathcal{A}, b \in \mathcal{B}\}, \tag{4}$$

where the addition is performed using the GF(q) arithmetic. That is, the set $\mathcal{A} + \mathcal{B}$ contains all pairwise sums of elements taken from $\mathcal{A}$ and $\mathcal{B}$. The CTV message from check node $\mathtt{c}$ to variable node $\mathtt{v}$ is then:

$$\mathrm{CTV}_{\mathtt{c}\to\mathtt{v}}^{(l)} = \sum_{\mathtt{v}'\in\{\mathcal{N}(\mathtt{c})\setminus\mathtt{v}\}} \left(\frac{h_{\mathtt{c},\mathtt{v}'}}{h_{\mathtt{c},\mathtt{v}}}\right) \cdot \mathrm{VTC}_{\mathtt{v}'\to\mathtt{c}}^{(l-1)}, \tag{5}$$

where the sum is a sumset operation and the multiplications are performed element-wise. Once all the CTV messages are calculated, the VTC messages are calculated as the *intersection* of the channel-information set and the incoming CTV message sets:

$$\mathrm{VTC}_{\mathtt{v}\to\mathtt{c}}^{(l)} = \mathrm{VTC}_{\mathtt{v}}^{(0)} \bigcap \left\{ \bigcap_{\mathtt{c}'\in\{\mathcal{N}(\mathtt{v})\setminus\mathtt{c}\}} \mathrm{CTV}_{\mathtt{c}'\to\mathtt{v}}^{(l)} \right\}. \tag{6}$$

A decoding failure occurs if unresolved variable nodes (i.e., containing sets with more than one symbol) remain after the decoder terminates.

III. Structural Properties of Exchanged Messages

In this section, we show that the VTC and CTV messages admit structural properties that facilitate iterative-decoding performance analysis. Denote the additive group of GF(q) by GF$^+$(q). We will see that to analyze the probability of decoding failure, it suffices to consider messages that are subgroups of GF$^+$(q). Assuming the all-zero codeword, the decoding process starts with the channel-information sets $\mathcal{M}_0^j$ as *channel subgroups*, which evolve into more general subgroups in the message-passing process. We start with two fundamental properties of the sumset and intersection operations between *cosets* of subgroups. Note that sums involving sets are interpreted as sumsets (see (4)).

Lemma 2. *Consider two subgroups $\mathcal{H}_a, \mathcal{H}_b$ of GF$^+$(q) and two cosets $\mathcal{H}_a + g_a$ and $\mathcal{H}_b + g_b$ for some $g_a, g_b \in$ GF$^+$(q). Then*

$$(\mathcal{H}_a + g_a) + (\mathcal{H}_b + g_b) = (\mathcal{H}_a + \mathcal{H}_b) + (g_a + g_b). \tag{7}$$

In addition, if both cosets contain an element γ, then

$$(\mathcal{H}_a + g_a) \bigcap (\mathcal{H}_b + g_b) = \left(\mathcal{H}_a \bigcap \mathcal{H}_b\right) + \gamma. \tag{8}$$

Proof. The relation in (7) is due to the associativity of the field addition operation. In addition, the sumset of $\mathcal{H}_a + \mathcal{H}_b$ forms a group, due to the closure of $\mathcal{H}_a$ and $\mathcal{H}_b$. Thus, the right-hand side of (7) is a *coset* of $\mathcal{H}_a + \mathcal{H}_b$. To prove (8), note that if γ belongs to $\mathcal{H}_a + g_a$ (resp. $\mathcal{H}_b + g_b$) then $\mathcal{H}_a + g_a = \mathcal{H}_a + \gamma$ (resp. $\mathcal{H}_b + g_b = \mathcal{H}_b + \gamma$). An element μ lies in $(\mathcal{H}_a + g_a) \bigcap (\mathcal{H}_b + g_b) = (\mathcal{H}_a + \gamma) \bigcap (\mathcal{H}_b + \gamma)$ if and only if there are $h_a \in \mathcal{H}_a$ and $h_b \in \mathcal{H}_b$ such that $\mu = h_a + \gamma = h_b + \gamma$. This holds if and only if $\mu - \gamma = h_a = h_b$, meaning that $\mu - \gamma \in \mathcal{H}_a \bigcap \mathcal{H}_b$ or $\mu \in (\mathcal{H}_a \bigcap \mathcal{H}_b) + \gamma$. □

As a result of Lemma 2, the right-hand side of (7) is a coset of the group $\mathcal{H}_a + \mathcal{H}_b$ and the right-hand side of (8) is a coset of the group $\mathcal{H}_a \bigcap \mathcal{H}_b$. That is, the sumset and non-empty intersection operations between cosets result in cosets. Moreover, these operations can be performed between the underlying subgroups, followed by the addition of a constant. We leverage this observation to derive structural properties of the exchanged messages in the set iterative decoder.

Lemma 3. *The VTC and CTV messages exchanged in the QMBC iterative-decoding process are cosets of subgroups of GF$^+$(q).*

Proof. As we saw in Section II-B, the sets $\mathcal{M}_0^j$ ($j = 0, 1, ..., s$) are mapped to *subgroups* of GF$^+$(q). More generally, the channel-information sets $\mathcal{M}_x^j$ for $x \in \mathcal{X}$ are mapped to *cosets* of these subgroups. Denote by $x_{\mathtt{v}}$ the correct codeword symbol at a certain variable node $\mathtt{v}$. The CTV message from an adjacent check node $\mathtt{c}$ to $\mathtt{v}$ at iteration 1 has the form (see (5))

$$\sum_{\mathtt{v}'\in\{\mathcal{N}(\mathtt{c})\setminus\mathtt{v}\}} \left(g_{\mathtt{v}'} \cdot \mathcal{M}_0^{j_{\mathtt{v}'}} + g_{\mathtt{v}'} \cdot x_{\mathtt{v}'}\right), \tag{9}$$

where for each $\mathtt{v}' \in \{\mathcal{N}(\mathtt{c})\setminus\mathtt{v}\}$, $g_{\mathtt{v}'}$ is a constant determined by the graph edge labels and $2^{j_{\mathtt{v}'}}$ is the cardinality of the channel-information set at $\mathtt{v}'$. For each $\mathtt{v}'$, the set $g_{\mathtt{v}'} \cdot \mathcal{M}_0^{j_{\mathtt{v}'}}$ is a subgroup of $\mathrm{GF}^+(q)$, where closure follows from the closure of the subgroup $\mathcal{M}_0^{j_{\mathtt{v}'}}$. Therefore, (9) is a sumset of cosets, resulting in a coset (see the first part of Lemma 2).

Recall that the correct codeword symbol $x_\mathtt{v}$ is contained in any CTV message to $\mathtt{v}$, as the channel may introduce partial erasures but no errors. Thus, the sumset of cosets (9) can be written as

$$\left(\sum_{\mathtt{v}' \in \{\mathcal{N}(\mathtt{c}) \setminus \mathtt{v}\}} g_{\mathtt{v}'} \cdot \mathcal{M}_0^{j_{\mathtt{v}'}} \right) + x_\mathtt{v}. \tag{10}$$

The VTC message at iteration 1 from $\mathtt{v}$ to $\mathtt{c}$ is the intersection between the channel-information set at $\mathtt{v}$ and the CTV message sets from $\{\mathcal{N}(\mathtt{v}) \setminus \mathtt{c}\}$ to $\mathtt{v}$. Both types of sets were shown above to be cosets, and all of them contain the correct codeword symbol $x_\mathtt{v}$. According to the second part of Lemma 2, the intersection between these cosets is a coset. Repeating the arguments above for the next decoding iterations, an invariant is maintained that the VTC and CTV messages are cosets of subgroups of $\mathrm{GF}^+(q)$. □

In the following theorem, we provide an important simplification for iterative-decoding performance analysis.

Theorem 4. *The probability of decoding failure is independent of the transmitted codeword. Furthermore, if the all-zero codeword was transmitted, the exchanged messages are subgroups of GF$^+(q)$.*

Proof. We formally prove the intuitive fact that decoding progress only depends on the underlying *subgroups* exchanged in the messages, and not on which cosets of these subgroups are exchanged. A VTC message from variable node $\mathtt{v}$ depends on the intersection of cosets as in (10). However, an intersection of cosets is a coset of the intersection of the underlying subgroups (Lemma 2). Thus, the *cardinality* of the VTC message depends on the underlying subgroups $\mathcal{M}_0^{j_\mathtt{v}}$ only. In other words, it depends on the *partial-erasure pattern*, i.e., on the cardinalities of the channel-information sets. Thus, the VTC message cardinalities are *independent* of the actual transmitted codeword.

A decoding failure occurs if a variable node set cardinality is larger than one at the end of the decoding process (recall that the correct symbol is always contained in the messages). Thus, the probability of decoding failure is independent of the transmitted codeword. If the all-zero codeword is transmitted, $x_\mathtt{v}$ in (10) are all zero. Thus, the CTV messages are obtained as a sumset of *subgroups*, resulting in subgroups. As a consequence, the intersection operation at variable nodes is performed between subgroups, resulting in subgroups as well. □

The size of the space of possible messages passed in the iterative-decoding process provides a measure of complexity of the iterative decoder. Due to Theorem 4, this size is upper bounded by the number of subgroups of $\mathrm{GF}^+(q)$. This is an important property of the iterative decoder that facilitates performance analysis, as we show next that the number of subgroups is much smaller compared to number of possible subsets.

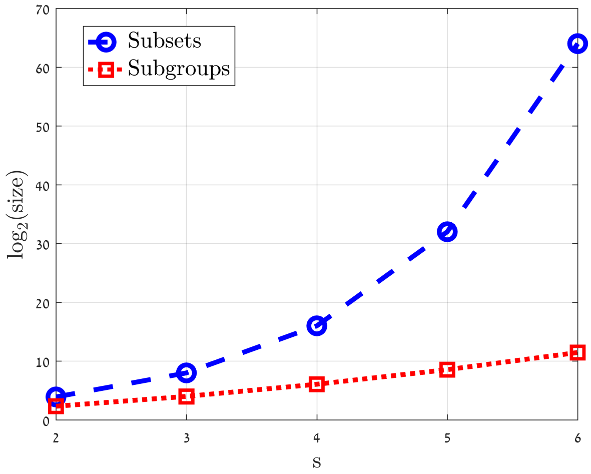


Fig. 1: A comparison of the number of subgroups of $\mathrm{GF}^+(q)$ and the number of non-empty subsets of $\mathrm{GF}^+(q)$, measured in bits.

Theorem 5. *The number of possible VTC and CTV messages passed in the decoding process, assuming that the all-zero codeword was transmitted, is upper bounded by*

$$T = \sum_{j=0}^{s} \left(\frac{\prod_{i=1}^{j} \left(2^s - 2^{i-1}\right)}{\prod_{i=1}^{j} \left(2^j - 2^{i-1}\right)} \right), \tag{11}$$

which is the number of subgroups of GF$^+(q)$.

Note that the number of subgroups of $\mathrm{GF}^+(q)$ of cardinality 2^j is the j^{th} summand in (11), which is the Gaussian coefficient $\binom{s}{j}_2$. The proof of Theorem 5 is based on representing $\mathrm{GF}^+(q)$ as an s-dimensional vector space over GF(2). Then, the number of subgroups of order 2^j is found as the number of subspaces of dimension 2^j (see e.g. [13] for the details). We remark that the actual number of subgroups exchanged in the decoding process (assuming that the all-zero codeword was transmitted) is not necessarily T. Instead, it depends on the channel information and on the edge labels. As an example, the only possible subgroups in the full-erasure case (i.e., if the only non-zero partial-erasure probability is ε_s) are $\mathcal{M}_0^0 = \{0\}$ and $\mathcal{M}_0^s$, where the latter set contains all the field elements.

We compare the number of subgroups of $\mathrm{GF}^+(q)$ to the number of non-empty subsets of $\mathrm{GF}^+(q)$ in Figure 1 (in logarithmic scale). This figure reveals the importance of the QMBC iterative-decoder structure to the analysis feasibility, by which the number of subgroups is orders of magnitude smaller compared to the number of subsets of $\mathrm{GF}^+(q)$. Hence performing density-evolution analysis for the QMBC is orders of magnitude less complex than for a general channel in the class of partial-erasure channels.

IV. The QMBC Decoding Threshold Region

To evaluate the performance of the iterative decoder, we use the density evolution method [14]–[16]. In this method, the probabilities of the exchanged messages as a function of the decoding iteration are tracked. The code length is assumed to be sufficiently large, such that the exchanged messages are statistically independent with high probability [14]. Let us consider a Tanner graph drawn uniformly at random out of the graphs with certain degree distributions $\lambda(x)$ and $\rho(x)$. The transmission of the all-zero codeword is assumed (see Theorem 4), such that the possible messages are subgroups of GF$^{+}(q)$. We denote these subgroups by $\{\mathcal{H}_t\}_{t=1}^{T}$ (recall that T is provided in (11)). For convenience, we assume that $\mathcal{H}_1 = \mathcal{M}_0^0 = \{0\}$.

Example 3. Consider the representation of GF(4) in Example 2. There are $T = 5$ subgroups of GF$^{+}(4)$, which can be ordered as follows: $\mathcal{H}_1 = \{0\}$, $\mathcal{H}_2 = \{0,1\}, \mathcal{H}_3 = \{0,\alpha\}, \mathcal{H}_4 = \{0,\alpha+1\}$ and $\mathcal{H}_5 = \{0,1,\alpha,\alpha+1\}$.

To obtain the QMBC density-evolution equations, we define $w_t^{(l)}$ (resp. $z_t^{(l)}$) as the probability that a CTV (resp. VTC) message at iteration l is $\mathcal{H}_t$. We denote by $\mathcal{R}_{i-1}$ an ordered list containing $i-1$ subgroup indices taken from $\{1,2,...,T\}$. These subgroups are interpreted as VTC (resp. CTV) messages to a check (resp. variable) node of degree i.

Example 4. Assume that $q = 4$ (i.e., $T = 5$ subgroups) and consider the $(3,6)$ LDPC code ensemble. Then $\mathcal{R}_2$ can be one of the ordered lists $[1,1], [1,2], \ldots, [5,5]$. Similarly, $\mathcal{R}_5$ can be one of the ordered lists $[1,1,1,1,1]$, $[1,1,1,1,2]$,. . .,$[5,5,5,5,5]$.

In the case of binary LDPC codes, the edge labels of a Tanner graph are simply '1's. In the GF(q) case, they are taken from the non-zero field elements. Thus, a GF(q) LDPC ensemble is characterized by an edge-label distribution in addition to the degree distributions. Let us denote the edge-label probability distribution by $\mathbb{L}$. We define $P_t(\mathcal{M}_{i-1}, \mathbb{L})$ as the probability of $\mathcal{H}_t$ as a CTV message, given the VTC messages indexed in $\mathcal{R}_{i-1}$, and the distribution $\mathbb{L}$. We also define $I_{t,j}(\mathcal{R}_{i-1})$ as an indicator function, which equals 1 if the intersection of the CTV messages indexed in $\mathcal{R}_{i-1}$ and the channel-information set $\mathcal{M}_0^j$ is the VTC message $\mathcal{H}_t$. Otherwise, $I_{t,j}(\mathcal{R}_{i-1})$ is 0 (note that the calculation of $I_{t,j}$ is independent of the edge labels). The following density-evolution equations are obtained:

$$w_t^{(l)} = \sum_{i=2}^{d_c} \rho_i \sum_{\mathcal{R}_{i-1}} \left(\prod_{m \in \mathcal{R}_{i-1}} z_m^{(l-1)} \right) \cdot P_t(\mathcal{R}_{i-1}, \mathbb{L}), \quad (12)$$

$$z_t^{(l)} = \sum_{i=2}^{d_v} \lambda_i \sum_{j=0}^{s} \varepsilon_j \sum_{\mathcal{R}_{i-1}} \left(\prod_{m \in \mathcal{R}_{i-1}} w_m^{(l)} \right) \cdot I_{t,j}(\mathcal{R}_{i-1}), \quad (13)$$

where the summation over $\mathcal{R}_{i-1}$ is understood over all the ordered lists containing $i-1$ subgroup indices taken from $\{1,2,...,T\}$. The initial conditions of the density-evolution equations (12)-(13) are determined by the transition probabilities in (1). That is, for each t such that $\mathcal{H}_t = \mathcal{M}_0^j$ $(j = 0,1,...,s)$, $z_t^{(0)}$ is initialized to ε_j. For example, if $q = 4$ and the subgroups are numbered as in Example 3, then $z_1^{(0)} = \varepsilon_0$, $z_2^{(0)} = \varepsilon_1$, $z_5^{(0)} = \varepsilon_2$ and $z_3^{(0)} = z_4^{(0)} = 0$. The asymptotic probability of decoding failure at iteration l, denoted $P_{\text{error}}^{(l)}$, is the probability that a VTC message at iteration l is not $\mathcal{H}_1 = \{0\}$:

$$P_{\text{error}}^{(l)} = \sum_{i=2}^{T} z_i^{(l)} = 1 - z_1^{(l)}. \quad (14)$$

The QMBC is characterized by multiple partial-erasure probabilities $\{\varepsilon_j\}_{j=1}^{s}$ rather than by a single erasure probability (as in the BEC or the QEC). Thus, we define the *QMBC decoding threshold region* by extending the BEC decoding threshold [7]. First, define the following *QMBC* $\mathbb{L}$*-region* for given $(\lambda(x), \rho(x))$ degree-distribution pair and edge-label distribution $\mathbb{L}$

$$\Omega_{\mathbb{L}}(\lambda,\rho) = \left\{ \varepsilon_1, \varepsilon_2, ..., \varepsilon_s \in [0,1]^s : \lim_{l\to\infty} P_{\text{error}}^{(l)}(\mathbb{L}) = 0 \right\}. \quad (15)$$

That is, an $\mathbb{L}$-region contains the partial-erasure probabilities leading asymptotically to zero probability of decoding failure under the edge-label distribution $\mathbb{L}$. The QMBC decoding-threshold region is the union of the QMBC $\mathbb{L}$-regions over all possible choices of $\mathbb{L}$:

$$\Omega(\lambda,\rho) = \bigcup_{\mathbb{L}} \Omega_{\mathbb{L}}(\lambda,\rho). \quad (16)$$

If both the boundaries of $\Omega(\lambda,\rho)$ and $\Omega_{\mathbb{L}}(\lambda,\rho)$ contain the same certain point, we say that $\mathbb{L}$ is *optimal* with respect to this point.

A. Optimal edge-label distributions

As mentioned earlier, GF(q) LDPC code ensembles are characterized by edge-label probability distributions in addition to degree distributions. In the following theorem, it is demonstrated that a poor selection of label distribution may degrade performance to that of a much worse channel. Denote by ε_{BEC} the decoding threshold of the BEC (or QEC) for a given degree-distribution polynomial pair $\lambda(x)$ and $\rho(x)$.

Theorem 6. *If the edge-label distribution* $\mathbb{L}$ *is chosen such that one of the non-zero GF(q) elements appears with probability* 1 *(i.e., all the labels are the same), then*

$$\Omega_{\mathbb{L}}(\lambda,\rho) = \left\{ \varepsilon_1, \varepsilon_2, ..., \varepsilon_s \in [0,1]^s : \sum_{j=1}^{s} \varepsilon_j \le \varepsilon_{\text{BEC}} \right\}. \quad (17)$$

That is, when the labels are all the same, a partial erasure is asymptotically equivalent to a full erasure, which is an undesired property. The key observation in proving this theorem is that messages exchanged in this case are restricted to the channel information messages (i.e., to the initial subgroups $\mathcal{M}_0^j$). Thus, the only way to get cardinality-1 intersection at a variable node is when a neighbouring check node has all its other neighbours with cardinality 1, same as when decoding over the BEC. The details are provided in Appendix A. As an immediate consequence of Theorem 6, simply taking binary ensembles (where the edge labels are all '1') with good performance (e.g., BEC capacity-achieving) necessarily gives poor performance over the QMBC.

In the following, we derive explicitly *optimal* $\mathbb{L}$ distributions for key points of interest in the QMBC decoding threshold region. For the derivation, we assume that the only non-zero partial-erasure probability is $\varepsilon_{j_{\max}}$, where $j_{\max}$ divides s. This choice does not mean that we are only interested in correcting partial erasures of type $j_{\max}$, but rather that we want to analyze the case when these are the dominant type of erasures (that is, when $\varepsilon_{j_{\max}}$ is considerably larger than any $\varepsilon_{j\neq j_{\max}}$). With this restriction we show that the multi-dimensional density-evolution equations (12)-(13) collapse to a single-letter density evolution where the only possible erasure type throughout decoding is the set $\mathcal{M}_0^{j_{\max}}$. With additional types of channel erasures there is need to track multiple erasure types in density evolution, and thus future optimality results are potentially more involved.

We assume a polynomial basis of GF(q), where $\mathcal{M}_0^j$ (for $j = 0, 1, ..., s$) contains all the polynomials of degree at most $j-1$ with coefficients in GF(2). These polynomials are evaluated at a primitive element of GF(q), denoted α. In this case, a basis to GF(q) over GF(2) is $\{1, \alpha, \alpha^2, ..., \alpha^{s-1}\}$.

Theorem 7. *Consider a QMBC with partial erasures of type $j_{\max}$ only, where $j_{\max}$ divides s. Then choosing $\mathbb{L}$ as the uniform distribution on $\left\{\alpha^{t\cdot j_{\max}}\right\}_{t=0}^{s/j_{\max}-1}$ is optimal with respect to achieving capacity.*

Proof. Suppose that the edge labels are taken from $\left\{\alpha^{t\cdot j_{\max}}\right\}_{t=0}^{s/j_{\max}-1}$. Denote the probability that a variable node is partially erased to $\mathcal{M}_0^{j_{\max}}$ at iteration l by y_l, and recall that $y_0 = \varepsilon_{j_{\max}}$. Suppose that the VTC messages at iteration $l \geq 0$ are either $\{0\}$ or $\mathcal{M}_0^{j_{\max}}$. We show by induction that the possible VTC messages at iteration $l+1$ remain $\{0\}$ or $\mathcal{M}_0^{j_{\max}}$. We first observe that a CTV message to a variable node at iteration l has a non-trivial intersection with $\mathcal{M}_0^{j_{\max}}$ (i.e., containing a non-zero element) if and only if at least one of the incoming VTC messages is a partial erasure *and* the label on this incoming VTC message edge is the same as the label on the outgoing CTV message edge. To see that, note that if the labels are the same, then $\mathcal{M}_0^{j_{\max}}$ is an argument in the CTV sumset operation (see (5)), whose result must contain $\mathcal{M}_0^{j_{\max}}$. Conversely, if edges from all partially-erased variable nodes have labels different from the label h to the target variable node, we show that the CTV message intersects with $\mathcal{M}_0^{j_{\max}}$ only on $\{0\}$. Take an edge label h_i of one partially-erased variable node. The labels $h, h_i \in \left\{\alpha^{t\cdot j_{\max}}\right\}_{t=0}^{s/j_{\max}-1}$ as monomials in α have degrees separated by at least $j_{\max}$. That means $h \cdot \mathcal{M}_0^{j_{\max}}$ and $h_i \cdot \mathcal{M}_0^{j_{\max}}$ intersect only on the 0 polynomial. This is true for all i, and thus any sum $\sum_i h_i \cdot x_i$, where x_i's are elements from $\mathcal{M}_0^{j_{\max}}$ not all zero, gives a polynomial not in $h \cdot \mathcal{M}_0^{j_{\max}}$. Equivalently, the CTV message intersects with $\mathcal{M}_0^{j_{\max}}$ only on the symbol 0. The intersection with $\{0\}$ or $\mathcal{M}_0^{j_{\max}}$ at the variable nodes completes the induction step.

Now by choosing $\mathbb{L}$ as the uniform distribution on $\left\{\alpha^{t\cdot j_{\max}}\right\}_{t=0}^{s/j_{\max}-1}$, each label has probability $j_{\max}/s$, and by the argument above a CTV message contains $\mathcal{M}_0^{j_{\max}}$ with probability

$$\sum_{i=2}^{d_c} \rho_i \left(1 - \left(1 - y_l \frac{j_{\max}}{s}\right)^{i-1}\right) = 1 - \rho\left(1 - \frac{y_l}{s/j_{\max}}\right). \tag{18}$$

The product $y_l \frac{j_{\max}}{s}$ is the probability that both "bad" events happen: the variable node connected by the incoming edge is partially erased (with probability y_l), and its edge has the same label as the one on the outgoing edge (with probability $\frac{j_{\max}}{s}$). The two events are statistically independent hence the product. A variable node remains partially-erased at iteration $l+1$ if and only if it was partially-erased initially (with probability $\varepsilon_{j_{\max}}$), and all its incoming CTV messages contain $\mathcal{M}_0^{j_{\max}}$. This leads to the *single-letter* recurrence relation

$$y_{l+1} = \varepsilon_{j_{\max}} \cdot \lambda \left(1 - \rho\left(1 - \frac{y_l}{s/j_{\max}}\right)\right). \tag{19}$$

The expression in (19) is the same recurrence equation as the BEC/QEC density evolution, only with y_l divided by $s/j_{\max}$ in the argument of $\rho(x)$. That is, we obtained a QMBC decoding threshold that is $s/j_{\max}$ times the BEC/QEC threshold for the same ensemble (when $\varepsilon_{j_{\max}}$ is the only non-zero partial-erasure probability). This is optimal because a BEC/QEC capacity-achieving ensemble will give a capacity-achieving QMBC ensemble according to (2). □

We remark that as all finite fields of the same order are isomorphic, the basis elements in $\left\{\alpha^{t\cdot j_{\max}}\right\}_{t=0}^{s/j_{\max}-1}$ can always be mapped to basis elements in any other representation of GF(q). As a consequence of Theorem 7, we can calculate *explicitly* the threshold of the optimal label distribution for any code ensemble, for $j_{\max}$ and q values given in the theorem. We now demonstrate how the optimal edge-label distribution derived in Theorem 7 improves the decoding performance. Assume that $q = 4$ and partial erasures of type $j_{\max} = 1$. In Figure 2, the QMBC $\mathbb{L}$-region defined in (15) is plotted for the optimal distribution (solid line) and is compared to the uniform distribution on the non-zero field elements (dotted line), for the $(3, 6)$ LDPC code ensemble. The QMBC Shannon capacity region is plotted (dashed line) for reference.

For the optimal distribution, the lower-right corner is $\varepsilon_1 = 0.858$, double the QEC threshold 0.429, according to (19). At the upper-left corner ($\varepsilon_1 = 0$), both label distributions attain the same ε_2 threshold – identical to the standard QEC threshold for full erasures. While the optimal distribution is superior at the lower-right corner, we found by a closer look on the threshold values obtained in Figure 2 that the uniform distribution becomes superior (by a small margin) for $\varepsilon_2 \geq 0.194$. This hints that in general there is no single distribution $\mathbb{L}$ universally optimal for all combinations of $\{\varepsilon_j\}_{j=1}^s$.

It is an interesting fact that achieving optimality requires a label distribution that is *not* the uniform distribution on the

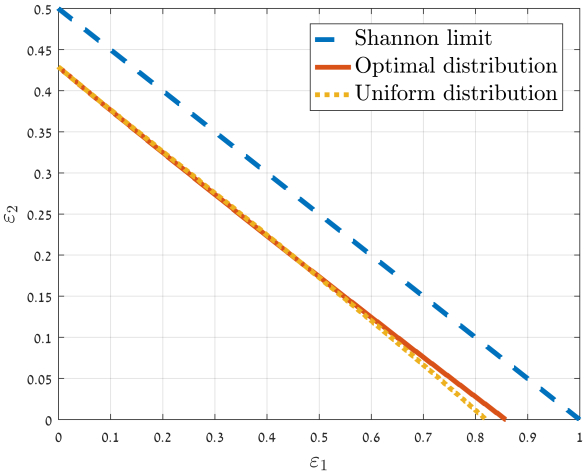


Fig. 2: The GF(4) QMBC $\mathbb{L}$-regions of two edge-label distributions for the $(3,6)$ LDPC code ensemble. The QMBC Shannon capacity region is plotted for reference.

non-zero field elements. We note that we can alternatively achieve optimality by using a binary capacity-achieving ensemble on $j_{\max}$ least significant bits of the symbols. However, the advantage of q-ary ensembles with an optimal edge-label distribution is that in addition to the optimality for $\varepsilon_{j_{\max}}$, the same code has good correction performance for infinitely many combinations of partial-erasure probabilities. There are several other ways by which some combination of binary codes can perform well over the QMBC, and even approach capacity in long block lengths. However, the advantage of designing q-ary QMBC LDPC codes is that one single code is directly optimized, and as we show in the sequel, that code-design algorithms for finite-length performance follow from the q-ary algebraic structure.

V. Edge-Labeling Algorithm for Improved Finite-Length Performance

In this section, we show how improved finite-length decoding performance is achieved by a wise labeling of the LDPC graph edges.

A. Stopping sets and local resolvability

A stopping set $\mathcal{S}$ is defined as a subset of variable nodes, such that all neighbours (check nodes) of $\mathcal{S}$ are connected to $\mathcal{S}$ at least twice. A key result in BEC finite-length iterative-decoding performance analysis is that the variable nodes in the maximal (fully) erased stopping set remain erased when the decoder stops [7], [8]. However, QMBC partially-erased variable nodes that belong to a stopping set might be eventually *resolved*. The reason is that with partial erasures the iterative decoder can make progress even if two or more neighbours of a check node are partially erased. This is demonstrated in the following example.

Example 5. Consider the Tanner graph in Figure 3, where the variable nodes $\mathtt{v}_1$ and $\mathtt{v}_2$ form a partially-erased stopping set ($q = 4$ is assumed). The initial CTV messages from the check node at the bottom are $\{0, h_2/h_1\}$ to $\mathtt{v}_1$ and $\{0, h_1/h_2\}$ to $\mathtt{v}_2$. If $h_1 = h_2$, the variable nodes are not resolved, as the intersection operation at variable nodes results in $\{0, 1\}$. Otherwise, they are resolved as $\{0\}$.

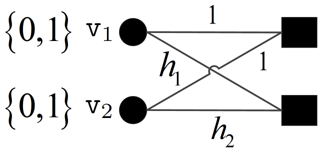


Fig. 3: $\mathtt{v}_1$ and $\mathtt{v}_2$ form a partially-erased stopping set (the channel information sets appear to the left). The resolvability of $\mathtt{v}_1$ and $\mathtt{v}_2$ depends on the values of h_1 and h_2.

As shown in Example 5, partially-erased variable nodes in a stopping set might be eventually resolved, depending on the edge-label configuration. However, non-resolved partial erasures must belong to a stopping set. Let us denote by $\mathcal{E}$ the set of partially-erased variable nodes.

Lemma 8. *The variable nodes that remain unresolved when the iterative QMBC decoder terminates belong to the maximum stopping set contained in $\mathcal{E}$.*

The proof of Lemma 8 is similar to the proof of [7, Lemma 3.140] and is omitted. Consider a check node connected to κ partially-erased variable nodes denoted $\mathtt{v}_1, \mathtt{v}_2, ..., \mathtt{v}_\kappa$, via edge labels $h_1, h_2, ..., h_\kappa$, respectively. We show that there are values of the edge labels such that a decoding progress is guaranteed, independently of information from any other variable node. Recall that in the full-erasure case (i.e., BEC or QEC), the local parity-check equation at a check node resolves at most one (full) erasure. However, it is possible to resolve *multiple* partial erasures in the QMBC case.

Definition 1. *The edge labels $h_1, h_2, ..., h_\kappa$ are said to be κ-resolvable if $\mathtt{v}_1, \mathtt{v}_2, ..., \mathtt{v}_\kappa$ are resolvable (i.e., decoded successfully), independently of other variable nodes.*

The motivation for Definition 1 is that by placing resolvable edge labels in stopping sets, improved decoding performance is expected. Let us denote by $j_{\max}$ the maximal partial-erasure type with non-zero probability. Consider the basis $\{1, \alpha, \alpha^2, ..., \alpha^{s-1}\}$ of GF(q) over GF(2) (see Section IV).

Theorem 9. *Consider a QMBC with partial-erasure types at most $j_{\max}$, where $j_{\max}$ divides s. The edge labels $\left\{\alpha^{t\cdot j_{\max}}\right\}_{t=0}^{s/j_{\max}-1}$ are $(s/j_{\max})$-resolvable for any set of $s/j_{\max}$ partially-erased variable nodes.*

Proof. Following the proof of Theorem 7, if h_i are distinct labels taken from $\left\{\alpha^{t\cdot j_{\max}}\right\}_{t=0}^{s/j_{\max}-1}$, the non-zero polynomials $h_i \cdot x_i$ of the variable nodes $\mathtt{v}_i$ have disjoint degrees, and thus can only satisfy the check equation if they are all zero. Hence the variable nodes can be resolved locally at the check node. □

Resolvable edge labels take advantage of the fact that a part of the q-ary symbol is not erased, or equivalently, that some of the bits in that symbol went through a noiseless channel. They essentially align the noiseless bit channels algebraically to get resolvability. What makes the use of resolvable edge labels interesting is that an edge-labeling algorithm will find (later in this section) the specific edges in the decoding graph that are particularly beneficial to align these noiseless bit channels.

B. Universal edge labeling

In addition to partial erasures of maximal type $j_{\max}$, a wider spectrum of partial erasures can be resolved when considering check nodes of degree 2. The resolvability of variable nodes connected to such check nodes is important, as every stopping set (in graphs without singly-connected variable nodes) is comprised of cycles that contain degree-2 check nodes [17]. As an example, the stopping set in Figure 3 is comprised of one cycle of length 4, with two check nodes of degree 2. This motivates finding edge labels that resolve QMBC partial erasures *universally*, that is, the same pair of labels will resolve any partial-erasure combination (j_1, j_2) satisfying $j_1+j_2 \leq s$. It turns out that universal edge labels exist for field sizes $q = 2^s$ with s up to (at least) $s = 13$. We provide a list of universal coefficients for up to $s = 6$ in Table I. In this table, α denotes a root of a primitive polynomial, such that the basis elements are $w_i = \alpha^{i-1}$ for $i = 1, 2, ..., s$ (see Section II-B). While non-binary LDPC codes are not likely to be used beyond these values of s, pairs of universally resolvable coefficients are implied for all *even* values s by [18, Theorem 1]. Finding universally resolvable edge labels in more generality (including for degrees more than 2) is an interesting algebraic problem, with broader relevance to applications such as RAID [19] and information dispersal [20].

C. Edge-labeling algorithm

Based on the existence of resolvable and universally-resolvable edge labels, we propose an edge-labeling algorithm for improved finite-length decoding performance. The idea is to distribute resolvable edge labels within edges of stopping sets such that partially-erased variable nodes are more likely to be resolved. Our proposal to solve QMBC stopping sets with an edge-labeling algorithm does not replace (and can be added on top) classical stopping-set mitigations through graph-level optimizations. Consider an LDPC graph with edge labels uniformly selected from the non-zero elements of GF(q). Suppose that the dominant partial-erasure type is $j_{\max}$, and that $j_{\max}$ divides s. If $j_{\max}$ does not divide s, then the maximal partial-erasure type (smaller than $j_{\max}$) that divides s is considered instead.

Algorithm 1. *(Edge labeling)*

1) Run the BEC iterative decoder with the channel parameter $\varepsilon = \varepsilon_{j_{\max}}$ for a predefined number of times. After each run, store the set of unresolved variable nodes.
2) Initialize Σ as the subgraph induced by the variable nodes from the sets of Step 1. Rank the variable nodes by their number of occurrences in the sets.
3) Modify the edge labels of check nodes of degree 2 connected to variable nodes in Σ to universal edge labels. Set the rank of connected variable nodes to 0.
4) Modify the edge labels of check nodes in Σ of degree larger than 2 but no larger than $s/j_{\max}$ to labels taken from $\left\{\alpha^{t \cdot j_{\max}}\right\}_{t=0}^{s/j_{\max}-1}$. Set the rank of connected variable nodes to 0.
5) Run over the sets found in Step 1 by ascending cardinality. For each check node connected to a set:
    a) Set κ' as the minimum between the number of non-zero ranking variable nodes and $s/j_{\max}$.
    b) Modify the κ' edge labels connected to non-zero highest-ranking variable nodes according to either Step 3 (if $\kappa' = 2$) or Step 4 (otherwise).

The steps of Algorithm 1 are explained as follows. First, we circumvent the hardness of finding stopping sets [21], [22] by running the BEC decoder, which fails on stopping sets. To focus on variable nodes that are likely to belong to a partially-erased stopping set, we rank the variable nodes according to their occurrences in the stopping sets found in Step 1. We construct the subgraph induced by the union of the sets found in Step 1, considered as a union of stopping sets, which is a stopping set as well. We then distribute either resolvable or universal edge labels for increased probability of local resolvability. Algorithm 1 assumes no prior information on the code graph structure and requires no topology changes. Specifically, one of its advantages is that the degree distributions are not affected.

As an alternative to Algorithm 1, one may consider to distribute resolvable edge labels on the graph edges (i.e., without concentrating on stopping sets). However, this will result in a Tanner graph with at most $s/j_{\max}+1$ edge label values instead of the possible $q-1 = 2^s-1$ edge labels. As a consequence, the probability of edge labels of the same value is increased, degrading the decoding performance (see Theorem 6). Thus, it is desired to first distribute the $q-1$ non-zero field elements uniformly on the edge labels and then to apply Algorithm 1 to stopping sets only. The performance improvement of Algorithm 1 is shown in Section VII.

VI. Finite-Length Analysis of Maximum-Likelihood Decoding

In this section, we analyze the finite-length decoding performance when a maximum-likelihood (ML) is used. We study the ML decoding performance for both the standard non-binary linear ensemble and LDPC ensembles. We denote by $\mathcal{E}_j$ $(j = 1, 2, ..., s)$ the index set of variable nodes partially-erased to $\mathcal{M}_0^j$ (see Section II), and define $\mathcal{E} \triangleq \bigcup_{j=1}^{s} \mathcal{E}_j$. We start with the following lemma.

Lemma 10. *Consider a linear code used for transmission over the QMBC. The probability of decoding failure under ML decoding is independent of the transmitted codeword.*

The proof of this lemma is provided in Appendix B. As a result of Lemma 10, we assume in the rest of this section the transmission of the all-zero codeword. Similarly to the BEC, an ML decoder fails when a codeword other than the all-zero

TABLE I: Universal cofficients for GF($q = 2^s$), $s = 2, 3, 4, 5, 6$.

s	Primitive polynomial	Universal coefficients
2	$x^2 + x + 1$	$\{1, \alpha\}$ or $\{1, 1 + \alpha\}$
3	$x^3 + x + 1$	$\{1, \alpha^2\}$ or $\{1, 1 + \alpha + \alpha^2\}$
4	$x^4 + x + 1$	$\{1, \alpha + \alpha^3\}$ or $\{1, \alpha^2 + \alpha^3\}$
5	$x^5 + x^2 + 1$	$\{1, 1 + \alpha^2 + \alpha^4\}$ or $\{1, \alpha + \alpha^3 + \alpha^4\}$
6	$x^6 + x + 1$	$\{1, 1 + \alpha^3 + \alpha^5\}$ or $\{1, 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^5\}$

codeword agrees with the partial-erasure pattern output by the channel. For analyzing ML decoding performance, we next define *consistent vectors* as the set of vectors that could have been the input to the channel given that the partial-erasure pattern $\{\mathcal{E}_j\}_{j=1}^s$ is observed.

Definition 2. *A GF(q) vector of length $|\mathcal{E}|$ is said to be consistent with respect to $\{\mathcal{E}_j\}_{j=1}^s$ if for $j = 1, 2, ..., s$ an element of this vector indexed in $\mathcal{E}_j$ is contained in $\mathcal{M}_0^j$.*

Example 6. Suppose $q = 4$, $\mathcal{E}_1 = \{1\}$ and $\mathcal{E}_2 = \{2\}$, and consider the representation of GF(4) as in Example 2. There are 8 consistent vectors with respect to $\mathcal{E}_1, \mathcal{E}_2$: $(0, 0)$, $(0, 1)$,$(0, \alpha)$, $(0, 1 + \alpha)$, $(1, 0)$, $(1, 1)$, $(1, \alpha)$ and $(1, 1 + \alpha)$.

A. Standard non-binary random ensemble

In this part we calculate the expected probability of ML decoding failure over the standard non-binary random ensemble (SNBRE) of linear codes. Each code in the SNBRE is defined by a parity-check matrix $\mathbf{H}$ of dimensions $(n - k) \times n$, whose entries are i.i.d. uniform random variables taken from the GF(q) elements. $\mathbf{H}_{\mathcal{E}}$ denotes its submatrix formed by the columns indexed in $\mathcal{E}$. That is, the columns corresponding to partially-erased variable nodes. To calculate the probability of decoding failure in the SNBRE case, we present the following definition. This definition uses the terminology of consistent vectors from Definition 2.

Definition 3. *The columns of $\mathbf{H}_{\mathcal{E}}$ are said to be partially linearly independent if no consistent vector apart from the zero vector exists in the null space of $\mathbf{H}_{\mathcal{E}}$.*

The partial linear independence definition reduces to the ordinary linear independence definition when the partial erasures are full erasures (i.e., only $\mathcal{E}_s$ is non empty). However, the columns of $\mathbf{H}_{\mathcal{E}}$ can be partially linearly independent even if they are not linearly independent under the ordinary definition (e.g., when there are more columns than rows). This is demonstrated in the following example.

Example 7. Consider the representation of GF(4) as in Example 2. Assume that $|\mathcal{E}_1| = 2$ (all the other $\mathcal{E}_j$ are empty), such that the columns of $\mathbf{H}_{\mathcal{E}}$ are $(1, 1)^T$ and $(\alpha, \alpha)^T$. These columns are linearly *dependent* (e.g., the vector $(\alpha, 1)^T$ is in the null space of $\mathbf{H}_{\mathcal{E}}$). However, there is no vector of length 2 with elements taken from $\mathcal{M}_0^1 = \{0, 1\}$ (with at least one non-zero element) in the null space of $\mathbf{H}_{\mathcal{E}}$. Therefore, the columns are partially linearly *independent* according to Definition 3.

To derive the probability of ML decoding success, we calculate the probability of partial linear independence. Let us define the set

$$\mathcal{M}_0^{j,j'} \triangleq \left\{ \frac{h_j}{h_{j'}} : h_j \in \mathcal{M}_0^j, h_{j'} \in \mathcal{M}_0^{j'} / \{0\} \right\}, \tag{20}$$

obtained by an element-wise division of the set $\mathcal{M}_0^j$ by $\mathcal{M}_0^{j'} / \{0\}$ (for certain $j, j' \leq s$). Further, define $\chi^{j,j'}$ as the cardinality of $\mathcal{M}_0^{j,j'}$:

$$\chi^{j,j'} \triangleq \left| \mathcal{M}_0^{j,j'} \right|. \tag{21}$$

Note that from group properties $\chi^{j,j'}$ is symmetric, i.e., $\chi^{j,j'} = \chi^{j',j}$. In addition, $\chi^{j,s} = q$ for any j.

Example 8. *Assume that $q = 4$. Then $\chi^{1,1} = 2$ and $\chi^{j,j'}$ for $j \neq 1$ or $j' \neq 1$ are 4.*

Let ψ denote the probability that the columns of a randomly drawn $\mathbf{H}_{\mathcal{E}}$ are partially linearly independent. For later use, we define $x^+ \triangleq \max(0, x)$.

Lemma 11. *Given $\{\mathcal{E}_j\}_{j=1}^s$, let $\mathcal{O}$ contain all vectors of length $|\mathcal{E}|$ in which j occurs $|\mathcal{E}_j|$ times. Then*

$$\psi \geq \max_{\boldsymbol{o} \in \mathcal{O}} \prod_{i=1}^{|\mathcal{E}|} \left(1 - \left(\prod_{l=1}^{i-1} \chi^{o_l, o_i} \right) / q^{n-k} \right)^+. \tag{22}$$

Proof. As the matrices in the SNBRE are equiprobable, ψ is a function of $\{|\mathcal{E}_j|\}_{j=1}^s$ rather than of $\{\mathcal{E}_j\}_{j=1}^s$. Let us concentrate on some fixed but arbitrary choice of index sets with cardinalities $\{|\mathcal{E}_j|\}_{j=1}^s$. This choice is represented by a vector $\boldsymbol{o}$ that contains j in indices of codeword symbols partially-erased to $\mathcal{M}_0^j$. Consider a matrix $\mathbf{H}_{\mathcal{E}}$ with columns $\boldsymbol{e}_i$ and denote by $\mathcal{A}_i$ the partial-erasure set indexed in o_i ($i = 1, 2, ..., |\mathcal{E}|$). We count in how many ways partially linearly independent columns can be placed in $\mathbf{H}_{\mathcal{E}}$.

Assume that the first $i' - 1$ columns of $\mathbf{H}_{\mathcal{E}}$ are partially linearly independent. The next column, $\boldsymbol{e}_{i'}$, must satisfy $\mathcal{A}_{i'} \cdot \boldsymbol{e}_{i'} \neq \sum_{l=1}^{i'-1} \mathcal{A}_l \cdot \boldsymbol{e}_l$. Thus, $\boldsymbol{e}_{i'}$ must be different from the vectors in $\Gamma = \sum_{l=1}^{i'-1} \mathcal{A}_l / \{\mathcal{A}_{i'} \setminus 0\} \cdot \boldsymbol{e}_l$. The number of elements in Γ is *upper bounded* by $\prod_{l=1}^{i'-1} \chi^{o_l, o_{i'}}$, as the linear combinations of $\boldsymbol{e}_l$ in Γ might not be distinct. This is since linear independence in the ordinary sense is not necessarily guaranteed. We maximize over $\boldsymbol{o} \in \mathcal{O}$ to tighten the bound, and to obtain a probability we normalize by $q^{(n-k)|\mathcal{E}|}$, which is the number of possible $\mathbf{H}_{\mathcal{E}}$ matrices. □

Apart from the lower bound on ψ of Lemma 11, there are cases where the *exact* value of ψ can be found. Consider a subset $\mathcal{J}^*$ of $\{1, 2, ..., s\}$ such that each element in $\mathcal{J}^*$ divides s and j' divides j for all $j, j' \in \mathcal{J}^*$, $j' \leq j$. We assume a representation of GF(q) (see Section II-B) such that for each $j^* \in \mathcal{J}^*$, the partial erasure set $\mathcal{M}_0^{j^*}$ is mapped to a *subfield* of GF(q) (i.e., in addition to being an additive subgroup of GF(q)). Moreover, for each pair $j, j' \in \mathcal{J}^*$, $j' \leq j$, $\mathcal{M}_0^{j'}$ is mapped to a subfield of $\mathcal{M}_0^{j}$.

Example 9. *If $q = 4$, the possible choices of $\mathcal{J}^*$ are $\{1\}$, $\{2\}$ and $\{1, 2\}$. If $q = 8$, $\mathcal{J}^*$ can be $\{1\}$, $\{2\}$, $\{1, 2\}$ or $\{1, 3\}$.*

The following lemma shows that when the divisibility conditions above are met, the upper bound on ψ via sequential exclusion of dependencies (Lemma 11) becomes exact, *if we sort the partial erasures in non-increasing order.*

Lemma 12. *Assume that $\mathcal{E}_j = \emptyset$ for $j \notin \mathcal{J}^*$. Denote by $\boldsymbol{o}$ the (now specific) vector of length $|\mathcal{E}|$ with s in its first $|\mathcal{E}_s|$ entries, $s-1$ in its next $|\mathcal{E}_{s-1}|$ entries downto 1 in its last $|\mathcal{E}_1|$ entries. Then*

$$\psi = \prod_{i=1}^{|\mathcal{E}|}\left(1-\left(\prod_{l=1}^{i-1} 2^{o_l}\right)/q^{n-k}\right)^{+}. \tag{23}$$

Proof. Consider the placement process depicted in the proof of Lemma 11 and assume that we place the i'th column. From the ordering of $\boldsymbol{o}$ we get that $\chi^{o_l,o_{i'}} = 2^{o_l}$ for $l < i'$. In choosing the vector $\boldsymbol{e}_{i'}$ we exclude all combinations of previous vectors $\boldsymbol{e}_l$ with coefficients in $\mathcal{M}_0^{o_l,o_{i'}}$. Assume by contradiction that two of these $\prod_{l=1}^{i'-1} 2^{o_l}$ combinations result in the same vector. But this would imply an $\boldsymbol{e}_{i''}$, $i'' < i'$, that is a combination of vectors $\boldsymbol{e}_l$, $l < i''$, with coefficients in $\mathcal{M}_0^{o_l,o_{i'}}$. Since for any l , $\mathcal{M}_0^{o_l,o_{i'}} = \mathcal{M}_0^{o_l,o_{i''}}$, this is a contradiction because it means that at step i'' we did not exclude all partially dependent vectors, and thus the count is exact with no over-subtraction. □

Based on either the lower bound on ψ of Lemma 11 or its exact value for the cases of Lemma 12, we calculate the expected value of $P^{\mathrm{ML}}_{\mathrm{error}}$ for the SNBRE.

Theorem 13. *The expected probability of decoding failure over codes drawn from the non-binary random ensemble under ML decoding is*

$$\begin{aligned}&\mathbb{E}_{\mathrm{SNBRE}}\left[P^{\mathrm{ML}}\left(\mathbf{H}\right)\right] && (24)\\ &\leq \sum_{\substack{|\mathcal{E}_0|,|\mathcal{E}_1|,\ldots,|\mathcal{E}_s|:\\ \sum_{j=0}^{s}|\mathcal{E}_j|=n}} \frac{n!}{|\mathcal{E}_0|!\,|\mathcal{E}_1|!\ldots|\mathcal{E}_s|!}\prod_{j=0}^{s}\varepsilon_j{}^{|\mathcal{E}_j|}\cdot\left(1-\tilde{\psi}\right),\end{aligned}$$

where $\tilde{\psi}$ is[1] *either the lower bound of Lemma 11, or its exact value in the cases of Lemma 12 (in the latter cases, an equality is attained in* (24)*).*

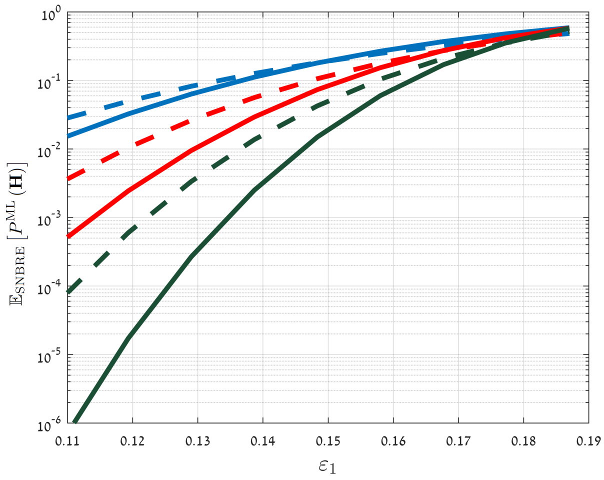


Fig. 4: Exact $\mathbb{E}_{\mathrm{SNBRE}}\left[P^{\mathrm{ML}}\left(\mathbf{H}\right)\right]$ as a function of ε_1, for $\varepsilon_2 = \varepsilon_1/10$ and $q = 4$ (solid lines). An asymptotically equivalent QEC with $\varepsilon = (3/5)\,\varepsilon_1$ is also shown (dashed lines). The codeword lengths are $n = 128, 256, 512$ (top to bottom) and the rate is $8/9$ (Shannon limit: 0.185).

Proof. Recall that the transmission of the all-zero codeword is assumed without loss of generality. Consider a fixed but arbitrary partial-erasure index sets $\{\mathcal{E}_j\}_{j=1}^{s}$. The channel output is not resolved as the all-zero codeword if and only if there is a non-zero consistent solution to $\mathbf{H}_{\mathcal{E}}\boldsymbol{x}_{\mathcal{E}}^{T} = \mathbf{0}$. This happens if the columns of $\mathbf{H}_{\mathcal{E}}$ are partially linearly independent, with probability which is $1 - \psi$. Finally, we sum over the possible cardinalities of the partial-erasure index sets, using the multinomial distribution and the channel partial-erasure probabilities, to obtain (24). □

If $s = 1$ and all the partial-erasure sets are $\{0, 1\}$ (i.e., BEC full-erasures), we obtain [8, Theorem 3.1] as a special case of Theorem 13 (with equality). In Figure 4 we plot $\mathbb{E}_{\mathrm{SNBRE}}\left[P^{\mathrm{ML}}\left(\mathbf{H}\right)\right]$ for a $q = 4$ channel with $\varepsilon_2 = \varepsilon_1/10$ and different n values. This is compared to an asymptotically equivalent q-ary erasure channel (QEC), i.e., with $\varepsilon = \varepsilon_1/2 + \varepsilon_2$. It is demonstrated that the QMBC finite-length ML performance is orders of magnitude better, though the Shannon limit is the same.

B. LDPC ensembles under ML decoding

In this part, we derive an upper bound on the expected ML decoding performance over the regular non-binary (d_v, d_c) LDPC ensemble. We start with the following lemma, which will serve us later in calculating the probability that a certain check node is satisfied.

Lemma 14. *Consider a vector $\boldsymbol{a}$ of length $m \geq 2$, whose entries are i.i.d. random variables uniformly distributed on the non-zero GF($q = 2^s$) elements. The probability that the entries of $\boldsymbol{a}$ sum to 0 is*

$$\Pr\left(\sum_{i=1}^{m} a_i = 0\right) = \frac{1-(1-q)^{1-m}}{q} \leq \frac{1}{q-1}. \tag{25}$$

[1] While implicit in the expressions, recall that $\tilde{\psi}$ depends on $\{|\mathcal{E}_j|\}_{j=1}^{s}$.

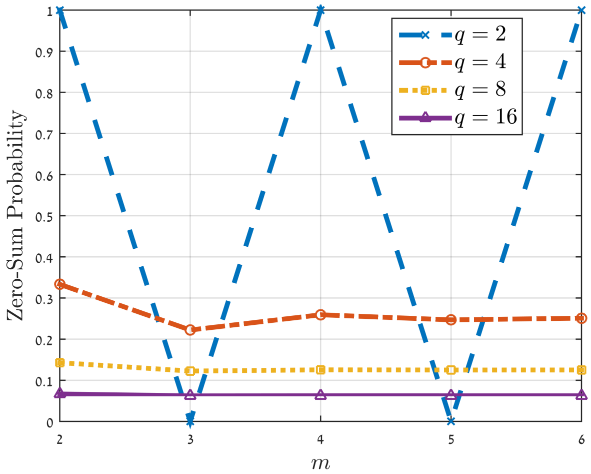


Fig. 5: The probability that a check node is satisfied given m non-zeros among its connected variable nodes, under the uniform distribution of the edge labels. The binary case ($q = 2$, no sensitivity to edge labels) is provided for reference.

The proof of this lemma is provided in Appendix C. In Figure 5, the zero-sum probability $\Pr\left(\sum_{i=1}^{m} a_i = 0\right)$ is shown for several values of m and q. Note that in the binary case ($q = 2$) this probability is 1 if m is even, and 0 otherwise, as expected. It is demonstrated in Figure 5 that the zero-sum probability is approximately independent of m when $q \geq 2$, and that the upper bound $1/(q-1)$ is tight. Note that $\Pr\left(\sum_{i=1}^{m} a_i = 0\right)$ depends on the number of non-zero entries in $\boldsymbol{a}$ and not on the entries themselves. In the following lemma, we calculate the number of consistent vectors (see Definition 2) with a certain number of non-zero entries.

Lemma 15. *Given $\mathcal{E} = \{\mathcal{E}_j\}_{j=1}^{s}$, the number of vectors with w non-zero entries that are consistent with $\mathcal{E}$ is*

$$\eta(w) = \sum_{\substack{\boldsymbol{u}: \sum_{j=1}^{s} u_j = w, \\ u_j \leq |\mathcal{E}_j|}} \prod_{j=1}^{s} \binom{|\mathcal{E}_j|}{u_j} \left(2^j - 1\right)^{u_j}. \tag{26}$$

Proof. An element u_j of $\boldsymbol{u}$ counts the number of non-zero entries taken from the $|\mathcal{E}_j|$ partial-erasure set $\mathcal{M}_0^j$. The number of ways to choose the locations of the partial-erasure sets is counted with the factor $\binom{|\mathcal{E}_j|}{u_j}$, where for each choice there are $\left(2^j - 1\right)^{u_j}$ ways to choose the non-zero entries. □

Note that when $s = 1$ and all the partial-erasure sets are $\{0, 1\}$ (i.e., BEC full-erasures), $\eta(w)$ degenerates into $\binom{|\mathcal{E}|}{w}$, which is the number of binary vectors of length $|\mathcal{E}|$ whose Hamming weight is w. Let us denote by $P^{\mathrm{ML}}(\mathcal{G})$ the probability of ML decoding failure for a certain Tanner graph $\mathcal{G}$ from the regular (d_v, d_c) ensemble. We now use Lemma 14 and Lemma 15 to upper bound the expected value (over graphs in the (d_v, d_c) ensemble) of $P^{\mathrm{ML}}(\mathcal{G})$. As in [8], [23], we use polynomial characteristic functions to identify graph configurations leading to failure events. We denote by $\operatorname{coef}\left(f(x), x^i\right)$ the ith coefficient f_i of x^i in the polynomial $f(x) = \sum_{i \geq 0} f_i x^i$ (note that $\operatorname{coef}\left((1+y)^n, x^k\right) = \binom{n}{k}$). We also denote by $\mathbb{E}_{\mathrm{LDPC}(d_v,d_c)}\left[P^{\mathrm{ML}}(\mathcal{G})\right]$ the expected probability of decoding failure, where the expectation is taken over LDPC codes in the (d_v, d_c) ensemble. Recall that $\eta(w)$ is a function of $\{|\mathcal{E}_j|\}_{j=1}^{s}$.

Theorem 16.

$$\mathbb{E}_{\mathrm{LDPC}(d_v,d_c)}\left[P^{\mathrm{ML}}(\mathcal{G})\right] \leq \tag{27}$$
$$\sum_{\substack{|\mathcal{E}_0|, |\mathcal{E}_1|, \ldots, |\mathcal{E}_s|: \\ \sum_{j=0}^{s} |\mathcal{E}_j| = n}} \frac{n!}{|\mathcal{E}_0|!\,|\mathcal{E}_1|! \ldots |\mathcal{E}_s|!} \prod_{j=0}^{s} \varepsilon_j^{|\mathcal{E}_j|}$$
$$\cdot \min\left\{1, \sum_{w=1}^{|\mathcal{E}|} \eta(w) \frac{\operatorname{coef}\left(\left((1+y)^{d_c} - 1 - y d_c\right)^{n \frac{d_v}{d_c}}, y^{w d_v}\right)}{\binom{n d_v}{w d_v}} \left(\frac{1}{q-1}\right)^{w \frac{d_v}{d_c}}\right\}.$$

Proof. An ML decoder fails if and only if there is a non-trivial solution to the equation $\mathbf{H}_{\mathcal{E}} \boldsymbol{x}_{\mathcal{E}}^T = \mathbf{0}$, which is consistent with respect to $\{\mathcal{E}_j\}_{j=1}^{s}$:

$$\Pr\left(\exists \boldsymbol{x}_{\mathcal{E}} \neq \mathbf{0}, \boldsymbol{x}_{\mathcal{E}} \text{ is consistent} : \mathbf{H}_{\mathcal{E}} \boldsymbol{x}_{\mathcal{E}}^T = \mathbf{0}\right) \tag{28}$$
$$\leq \sum_{\boldsymbol{x}_{\mathcal{E}} \neq \mathbf{0}, \boldsymbol{x}_{\mathcal{E}} \text{ is consistent}} \Pr\left(\mathbf{H}_{\mathcal{E}} \boldsymbol{x}_{\mathcal{E}}^T = \mathbf{0}\right),$$

where the upper bound follows by the union bound. Consider an arbitrary but fixed consistent vector $\boldsymbol{x}_{\mathcal{E}}$ and denote the number of its non-zero entries by $w(\boldsymbol{x}_{\mathcal{E}})$. There are $w(\boldsymbol{x}_{\mathcal{E}}) d_v$ edges connected to variable nodes corresponding to the non-zero elements of $\boldsymbol{x}_{\mathcal{E}}$. For $\mathbf{H}_{\mathcal{E}} \boldsymbol{x}_{\mathcal{E}}^T = \mathbf{0}$ to hold, each neighbouring check of the $w(\boldsymbol{x}_{\mathcal{E}})$ non-zero variable nodes must be connected to these variable nodes at least twice. As the total number of check nodes is $n d_v / d_c$, we have $\operatorname{coef}\left(\left((1+y)^{d_c} - 1 - d_c y\right)^{n \frac{d_v}{d_c}}, y^{w(\boldsymbol{x}_{\mathcal{E}}) d_v}\right)$ configurations out of $\binom{n d_v}{w(\boldsymbol{x}_{\mathcal{E}}) d_v}$ such configuration. According to Lemma 14, the probability that a certain check node is satisfied is upper bounded by $1/(q-1)$ (recall that uniform edge labels are assumed). The number of check nodes connected to $w(\boldsymbol{x}_{\mathcal{E}})$ variable nodes is at least $w(\boldsymbol{x}_{\mathcal{E}}) d_v / d_c$. Thus, $\left(1/\left(q-1\right)\right)^{w(\boldsymbol{x}_{\mathcal{E}}) d_v / d_c}$ is an upper bound on the probability that all check nodes connected to the $w(\boldsymbol{x}_{\mathcal{E}})$ non-zero variable nodes are satisfied. Finally, by summing over all the possible weights of consistent vectors (counted by $\eta(w)$ of Lemma 15) and taking into account the channel partial-erasure probabilities, (27) is obtained. The minimum in (27) is taken to tighten the upper bound. □

In Figure 6, we compare (27) for $q = 4$, where the set $\{0, 1\}$ is considered as either a partial erasure (decoded with the QMBC decoder) or a full erasure (decoded with the BEC decoder). In terms of the upper bound (27), the QMBC model is expected to provide ML decoding performance orders of magnitude better compared to full-erasure decoding.

VII. Simulation Results

In this part, we present simulation results of the QMBC iterative-decoding performance. We used the regular $(3, 27)$

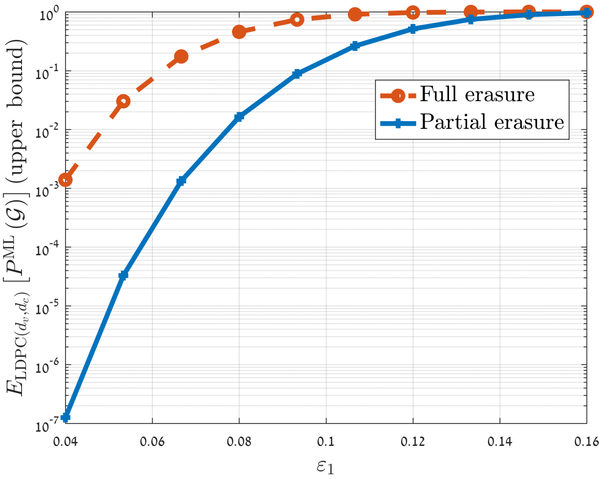
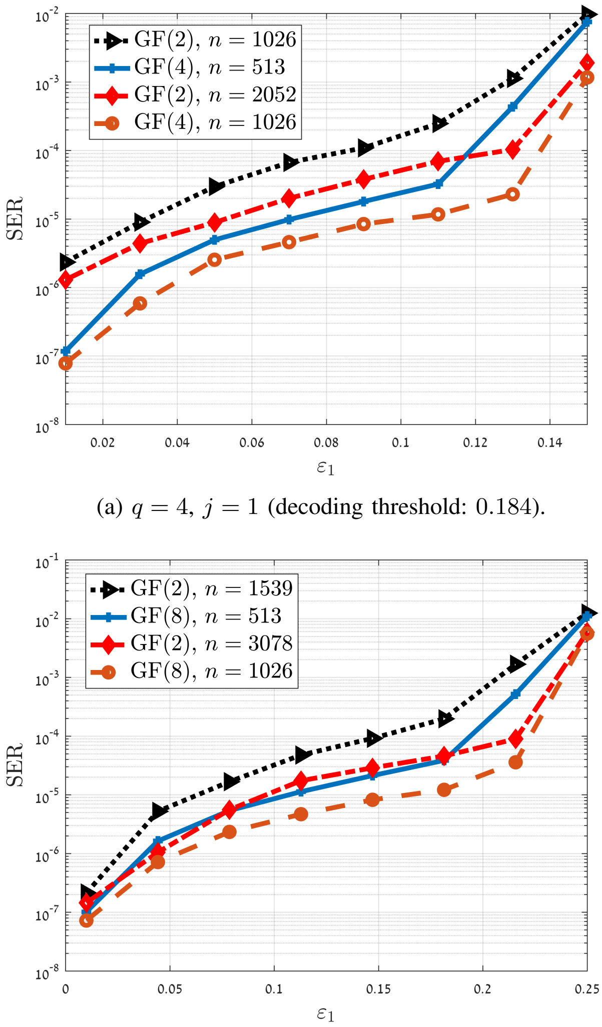


Fig. 6: A comparison of $\mathbb{E}_{\text{LDPC}(d_v,d_c)}\left[P^{\text{ML}}(\mathcal{G})\right]$ for the LDPC ensemble $(3,27)$ (rate $8/9$), for a GF(4) code of length 252. The set $\{0,1\}$ is either considered as a partial erasure or a full erasure with probability ε_1.

LDPC code ensemble (rate $8/9$), whose high rate is desired in memory and storage applications. Two codeword lengths were considered: $n = 513$ and $n = 1026$. The average decoding performance is measured by symbol erasure rate (SER), where each variable node that remains partially erased when the decoder terminates contributes to this quantity.

A. *Comparison to binary full erasures*

As a preliminary step, we considered binary coding with GF(q) symbols converted to bits. In this setting, a GF(q) symbol is decomposed into s bits, where a partial-erasure event of type j corresponds to j (fully) erased least significant bits. We compare GF(q) codes with partial erasures (decoded using the QMBC decoder) to binary codes with equivalent full erasures (decoded using the BEC decoder). The results are shown in Figure 7. It is demonstrated that partial-erasure decoding outperforms binary erasure decoding, offering SER performance better by up to an order of magnitude. The improved performance of GF(q) codes over binary codes is explained by the mitigated effect of stopping sets due to the non-binary edge labels, as we developed in Section V. We see that the performance gap diminishes as the codeword length is increased. The reason is that for sufficiently long codeword lengths, the probability of having a stopping set of a certain size gets smaller. Thus in long block lengths, binary codes are likely to offer competitive performance. However, stopping sets are still the cause of failure events in practical block lengths. In this section we do not consider the alternative (mentioned in Section IV) of using binary codes for the j upper bits only. While this alternative will likely outperform the plotted options on one specific value of j, it would completely collapse if there is even a tiny fraction of higher-order partial erasures.



(a) $q = 4$, $j = 1$ (decoding threshold: 0.184).

(b) $q = 8$, $j = 1$ (decoding threshold: 0.276).

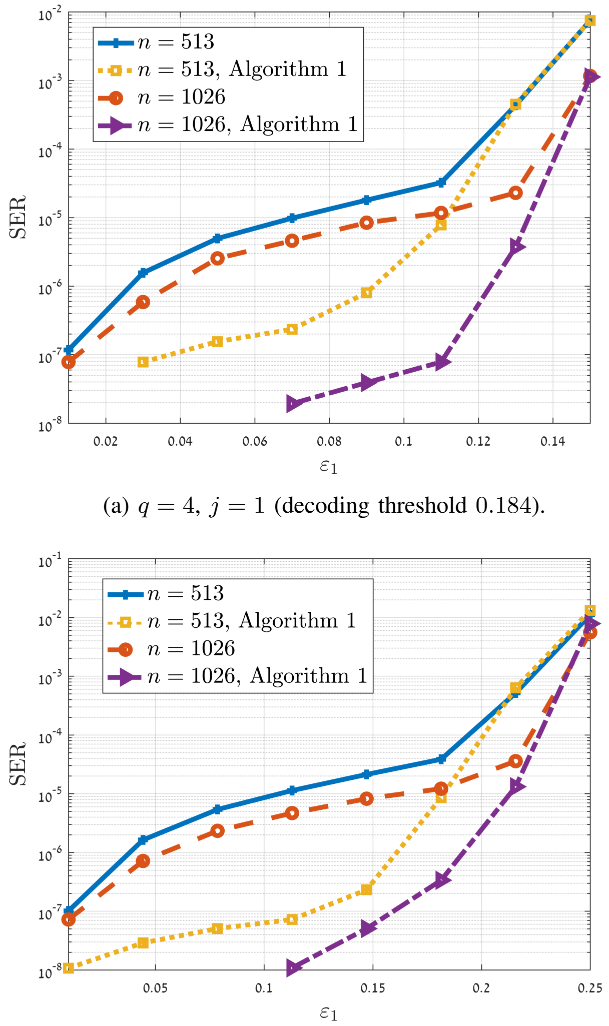
Fig. 7: SER performance comparison between GF(q) and binary codes. The labels of the GF(q) LDPC codes are uniformly distributed.

B. *Performance of the edge-labeling algorithm*

In this part, we show that the decoding performance of GF(q) LDPC codes can be further improved using the edge-labeling algorithm (Algorithm 1) developed in Section V-C. In Figure 8, we compare the iterative decoding performance of GF(q) with uniformly-distributed edge labels to edge labels optimized using Algorithm 1. The optimized edge labels lead to a significant improvement in in SER performance, up to two orders of magnitude. It is demonstrated that the performance gap increases with q for a fixed partial-erasure type. The reason is the larger number of resolvable edge labels, which increases with q (see Theorem 9).

VIII. Conclusion

This work offers a study of the performance of iterative decoding of GF(q) LDPC codes over the QMBC. By an asymptotic threshold analysis, we demonstrated explicitly how the edge label distribution affects decoding performance. We



(a) $q = 4$, $j = 1$ (decoding threshold 0.184).

(b) $q = 8$, $j = 1$ (decoding threshold 0.276).

Fig. 8: SER performance comparison of QMBC partial-erasure decoding, between uniformly-distributed and optimized edge labels. The decoding thresholds are given for optimal edge-label distributions.

later showed that unlike the binary case, partially-erased stopping sets can be resolved by a wise setting of edge labels. For this aim, we proposed and evaluated an edge-labeling algorithm for improved finite-length decoding performance. Finally, we derived expressions for the finite-length performance of a maximum-likelihood decoder, both for the standard non-binary random ensemble and for LDPC ensembles.

Our work leaves interesting problems for future research. Designing good GF(q) LDPC codes for the QMBC is an important research direction. Unlike binary codes, GF(q) LDPC codes require a joint optimization of degree and edge-label distributions. It is of importance to give an expression for the QMBC finite-length performance that depends on the edge-label distribution in addition to the stopping-set distribution. As another direction, the upper bound on the ML decoding performance for LDPC ensembles might be improved by considering non-uniform edge-label distributions.

Appendix A
Proof of Theorem 6

Assume that all the edge labels are the same. In this case, the CTV messages are independent of the edge labels, and we have (see (5)):

$$\mathrm{CTV}^{(l)}_{\mathtt{c}\to\mathtt{v}} = \sum_{\mathtt{v}'\in\{\mathcal{N}(\mathtt{c})\backslash\mathtt{v}\}} \mathrm{VTC}^{(l-1)}_{\mathtt{v}'\to\mathtt{c}}. \tag{29}$$

That is, an outgoing CTV message is simply the sumset of the incoming VTC messages. Recall that the initial channel-information sets are contained in each other, i.e. $\mathcal{M}_0^j \subseteq \mathcal{M}_0^{j'}$ for $j \leq j'$, and that each set is an additive subgroup of GF$^+(q)$, closed under addition. For example, the possible channel-information sets when $q = 4$ are $\{0\}, \{0,1\}$ and $\{0,1,2,3\}$ (we define $\mathcal{M}_0^0$ as the singleton $\{0\}$). Due to the closure property of subgroups, the initial sumset at a check node can be written as:

$$\sum_{j\in\mathcal{M}_\mathtt{v}} \mathcal{M}_0^j = \mathcal{M}_0^{\max\limits_{j\in\mathcal{M}_\mathtt{v}} j}, \tag{30}$$

where $\mathcal{M}_\mathtt{v}$ is an ordered list containing indices of incoming VTC messages (See Section IV). Thus, the sumset operation at check nodes simplifies to finding the incoming VTC message of the maximum cardinality. In a similar manner, the intersection operation performed at variable nodes simplifies to finding the incoming incoming CTV message of smallest cardinality:

$$\bigcap_{j\in\mathcal{M}_\mathtt{c}} \mathcal{M}_0^j = \mathcal{M}_0^{\min\limits_{j\in\mathcal{M}_\mathtt{c}} j}, \tag{31}$$

where $\mathcal{M}_\mathtt{c}$ is an ordered list containing indices of incoming CTV messages. As a result of (30) and (31), the QMBC decoder simplifies to the BEC decoder. That is, a CTV message is a partial erasure if any of the incoming VTC messages is a partial erasure and a VTC message is a partial erasure if the corresponding variable was initially partially erased and all incoming CTV messages are partial erasure. This leads to the BEC density-evolution equation with $\varepsilon = \sum_{j=1}^{s} \varepsilon_j$. □

Appendix B
Proof of Lemma 10

Assume the transmission of a codeword $\boldsymbol{c}$ from a linear code defined by a parity-check matrix $\mathbf{H}$. Let us denote by $\boldsymbol{x}^{(t)}$ ($t = 1, 2, ..., \prod_{j=1}^{s} |\mathcal{E}_j|$) the GF($q$) words (not necessarily codewords) consistent (see Definition 2) with the channel output $\boldsymbol{y}$. That is, any $\boldsymbol{x}^{(t)}$ as input would result in the output $\boldsymbol{y}$, given the partial-erasure index sets $\{\mathcal{E}_j\}_{j=1}^{s}$. An ML decoder fails if and only if there exists $\boldsymbol{x}^{(t)} \neq \boldsymbol{c}$, such that $\mathbf{H}\boldsymbol{x}^{(t)} = \mathbf{0}$. Now assume the transmission of the all-zero codeword, and recall that $\mathcal{M}_{c_i}^j = \mathcal{M}_0^j + c_i$ (see Section II-A). Then each $\boldsymbol{x}^{(t)}$ consistent with the sets $\mathcal{M}_{c_i}^j$ and satisfying $\mathbf{H}\boldsymbol{x}^{(t)} = \mathbf{0}$ has a corresponding $\boldsymbol{z}^{(t)} = \boldsymbol{x}^{(t)} - \boldsymbol{c}$ that is consistent with the sets $\mathcal{M}_0^j$ and satisfying $\mathbf{H}\boldsymbol{z}^{(t)} = \mathbf{0}$. Thus, the probability of decoding failure under ML decoding is independent of the transmitted codeword.

Appendix C
Proof of Lemma 14

Let us start with the case $m = 2$. The elements of the vector $\boldsymbol{a}$ sum to zero if and only if they are the same. Thus, there are $q-1$ vectors with all non-zero elements of length 2 whose elements sum to zero. As a consequence, there are $(q-1)^2 - (q-1)$ vectors with all non-zero elements whose elements sum to a non-zero field element. Let us move to the $m = 3$ case, where we consider a vector $\tilde{\boldsymbol{a}} = (\tilde{a}_1, \tilde{a}_2, \tilde{a}_3)$ of 3 non-zero elements. The equation $\tilde{a}_1 + \tilde{a}_2 + \tilde{a}_3 = 0$ is equivalent to $\tilde{a}_1 + \tilde{a}_2 = \tilde{a}_3$. As $\tilde{a}_3$ can be any non-zero field element, the number of ways to obtain $\tilde{a}_1 + \tilde{a}_2 + \tilde{a}_3 = 0$ is the same as the number of ways to obtain a non-zero sum of $\tilde{a}_1 + \tilde{a}_2$. According to the previous $m = 2$ result, this number is $(q-1)^2 - (q-1)$. Continuing in the same fashion, there are $\sum\limits_{i=1}^{m-1} (q-1)^i (-1)^{m-i-1}$ ways to obtain a zero sum for a random vector of m non-zero elements, $m \geq 2$. Simplifying the sum and normalizing by the number of possible vectors $(q-1)^m$ leads to (25). The upper bound in (25) is equivalent to $(1-q)^{2-m} \leq 1$, which holds for all $m \geq 2$. This upper bound is sharp, as it is attained with equality for $m = 2$.

References

[1] R. Cohen and Y. Cassuto, "Iterative decoding of LDPC codes over the q-ary partial erasure channel," *IEEE Transactions on Information Theory*, vol. 62, no. 5, May 2016.

[2] G. Ungerboeck, "Channel coding with multilevel/phase signals," *IEEE Transactions on Information Theory*, vol. 28, no. 1, pp. 55–67, Jan 1982.

[3] A. S. Avestimehr, S. N. Diggavi, and D. N. C. Tse, "A deterministic model for wreless relay networks an its capacity," in *2007 IEEE Information Theory Workshop on Information Theory for Wireless Networks*, July 2007, pp. 1–6.

[4] R. Gabrys, E. Yaakobi, and L. Dolecek, "Graded bit-error-correcting codes with applications to flash memory," *IEEE Transactions on Information Theory*, vol. 59, no. 4, pp. 2315–2327, April 2013.

[5] R. G. Gallager, "Low-density parity-check codes," *IRE Transactions on Information Theory*, vol. 8, no. 1, pp. 21–28, 1962.

[6] M. Davey and D. MacKay, "Low-density parity check codes over GF(q)," *IEEE Communications Letters*, vol. 2, no. 6, pp. 165–167, June 1998.

[7] T. Richardson and R. Urbanke, *Modern Coding Theory*. Cambridge University Press, 2008.

[8] C. Di, D. Proietti, I. Telatar, T. Richardson, and R. Urbanke, "Finite-length analysis of low-density parity-check codes on the binary erasure channel," *IEEE Transactions on Information Theory*, vol. 48, no. 6, pp. 1570–1579, Jun 2002.

[9] A. Bazarsky, N. Presman, and S. Litsyn, "Design of non-binary quasi-cyclic LDPC codes by ACE optimization," in *2013 IEEE Information Theory Workshop (ITW)*, Sept 2013, pp. 1–5.

[10] B. Amiri, J. Kliewer, and L. Dolecek, "Analysis and enumeration of absorbing sets for non-binary graph-based codes," *IEEE Transactions on Communications*, vol. 62, no. 2, pp. 398–409, February 2014.

[11] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Transactions on Information Theory*, vol. IT-27, pp. 533–547, 1981.

[12] T. C. Tao and V. H. Vu, *Additive Combinatorics*. Cambridge University Press, 2006.

[13] A. Prasad, "Counting subspaces of a finite vector space – 1," *Resonance*, vol. 15, no. 11, pp. 977–987, 2010.

[14] T. Richardson and R. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 599–618, 2001.

[15] V. Rathi and R. Urbanke, "Density evolution, thresholds and the stability condition for non-binary LDPC codes," *IEE Proceedings-Communications*, vol. 152, no. 6, pp. 1069–1074, Dec 2005.

[16] A. Bennatan and D. Burshtein, "Design and analysis of nonbinary LDPC codes for arbitrary discrete-memoryless channels," *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 549–583, 2006.

[17] T. Tian, C. Jones, J. D. Villasenor, and R. D. Wesel, "Construction of irregular LDPC codes with low error floors," in *IEEE International Conference on Communications*, May 2003, pp. 3125–3129.

[18] N. Raviv, Y. Cassuto, R. Cohen, and M. Schwartz, "Erasure correction of scalar codes in the presence of stragglers," in *2018 IEEE International Symposium on Information Theory (ISIT)*, June 2018.

[19] D. A. Patterson, G. Gibson, and R. H. Katz, "A case for redundant arrays of inexpensive disks (RAID)," in *Proceedings of the 1988 ACM SIGMOD International Conference on Management of Data*, ser. SIGMOD '88. New York, NY, USA: ACM, 1988, pp. 109–116.

[20] M. O. Rabin, "Efficient dispersal of information for security, load balancing, and fault tolerance," *J. ACM*, vol. 36, no. 2, pp. 335–348, Apr. 1989.

[21] A. McGregor and O. Milenkovic, "On the hardness of approximating stopping and trapping sets," *IEEE Transactions on Information Theory*, vol. 56, no. 4, pp. 1640–1650, April 2010.

[22] K. Krishnan and P. Shankar, "Computing the stopping distance of a tanner graph is NP-hard," *IEEE Transactions on Information Theory*, vol. 53, no. 6, pp. 2278–2280, June 2007.

[23] A. Orlitsky, K. Viswanathan, and J. Zhang, "Stopping set distribution of LDPC code ensembles," *IEEE Transactions on Information Theory*, vol. 51, no. 3, pp. 929–953, March 2005.

Rami Cohen received the B.Sc. in Electrical Engineering and Physics (*cum laude*) and the M.Sc. and Ph.D. in Electrical Engineering in 2012 and 2017, respectively, all from the Technion - Israel Institute of Technology. He is currently with Medtronic Israel, working on large-scale deep-learning algorithms for medical applications. His research interests include applications of coding theory and information theory tools to practical systems, such as high-speed memory devices.

Netanel Raviv (S'15–M'17) received a B.Sc. in mathematics and computer science in 2010, an M.Sc. and Ph.D. in computer science in 2013 and 2017, respectively, all from the Technion, Israel. He is now a postdoctoral scholar at the Center for the Mathematics of Information (CMI) at the California Institute of Technology. He is an awardee of the IBM Ph.D. fellowship for the academic year of 2015-2016, the first prize in the Feder family competition for best student work in communication technology, and the Lester-Deutsche Postdoctoral Fellowship. His research interests include applications of coding techniques to computation, storage, and networks.

Yuval Cassuto (S'02M'08SM'14) is a faculty member at the Viterbi Department of Electrical Engineering, Technion Israel Institute of Technology. His research interests lie at the intersection of the theoretical information sciences and the engineering of practical computing and storage systems. During 20102011 he has been a Scientist at EPFL, the Swiss Federal Institute of Technology in Lausanne. From 2008 to 2010 he was a Research Staff Member at Hitachi Global Storage Technologies, San Jose Research Center. He received the B.Sc degree in Electrical Engineering, summa cum laude, from the Technion in 2001, and the M.S. and Ph.D. degrees in Electrical Engineering from the California Institute of Technology, in 2004 and 2008, respectively. From 2000 to 2002, he was with Qualcomm, Israel R&D Center, where he worked on modeling, design and analysis in wireless communications. Dr. Cassuto has won the 2010 Best Student Paper Award in data storage from the IEEE Communications Society, as well as the 2001 Texas Instruments DSP and Analog Challenge $100,000 prize.