LDPC Codes for the q-ary Bit-Measurement Channel

Rami Cohen and Yuval Cassuto

The Viterbi Faculty of Electrical Engineering
Technion - Israel Institute of Technology
Technion City, Haifa 3200003, Israel
Email: rc@campus.technion.ac.il, ycassuto@ee.technion.ac.il

***Abstract*—In this paper, we introduce a new channel model we term the q-ary bit-measurement channel (QBMC). 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 by measuring a single bit from the symbol in each read step, starting from the most significant bit. An error event occurs when not all the symbol bits are known, e.g., due to a premature termination of the read sequence. To deal with such error events, we propose the use of GF(q) low-density parity-check (LDPC) codes and analyze their iterative-decoding performance. In particular, we show how to exploit the algebraic structure of the QBMC channel for efficient analysis, and study the effect of the Tanner graph's edge-label distribution on the decoding performance. It is shown that for $q = 4$ the optimal correction of single-bit erasures is achieved by a distribution different from the uniform distribution on the non-zero elements of GF(4).**

I. Introduction

The rapid development of memory technologies has introduced challenges to the continued scaling of memory devices in density and access speed. A memory device can be often modeled as a *measurement channel* with $q = 2^s$ voltage/current levels, each represented as s bits. As an example, there are eight voltage levels (i.e., $q = 8$) in a TLC (triple level cell) flash memory, where the levels are represented as three bits. Due to speed constraints, the read output may occasionally be needed before the read circuitry was able to read all the bits of the symbol. This results in an error event we call *partial erasure*.

In this work, we introduce the *q-ary bit-measurement channel* (QBMC) model for targeting natural partial-erasure errors in memory devices. In this model, the symbol bits are read sequentially, starting from the most significant bit (MSB) and providing the next significant bit at each measurement step. That is, the first measurement determines whether the symbol is known to belong to either the upper or lower $q/2$ symbols. The second measurement gives the upper or lower $q/4$ symbols within the previously obtained set of $q/2$ symbols, and so on. In an error event, the read process terminates before all the bits are measured. This leads to an output *set*, whose cardinality is a power of 2, of *consecutive* symbols containing the input symbol. In case the output set cardinality is larger than one, we say that a partial-erasure event occurred. This terminology was introduced previously in the q-ary partial erasure channel (QPEC) model [1]. However, in contrary to the random output sets in the QPEC model, the QBMC output sets are structured in the sense they contain consecutive symbols.

The multi-bit structure of multi-level memories has attracted some prior attention. For example, in [2] the error rates of the different TLC bits were analyzed and addressed. In [3], low-density parity-check (LDPC) codes were optimized to jointly correct errors in the high and low bits of 4-level cells, where in [4] LDPC codes were used for flash memories based on rank modulation. This study considers the use of GF(q) LDPC codes to deal with partial erasures, and contributes analytical insights to a central problem related to flash-memory reliability. The motivation to use LDPC codes is their low complexity of implementation and good performance under iterative decoding. We characterize structural properties of the messages passed in the iterative decoding process, using concepts taken from field theory and group theory. We then show that these properties lead to simplified asymptotic decoding performance analysis. To obtain a suitable measure of decoding performance, we generalize the binary erasure channel (BEC) decoding threshold [5], by defining the QBMC *decoding threshold region*. We then demonstrate the dependency of this region on the edge-label distribution of the Tanner graph representing the GF(q) LDPC code.

The paper is structured as follows. In Section II, the QBMC model and an iterative message-passing decoder are provided. Structural properties of the decoder are discussed in Section III. Performance analysis of the iterative decoder is provided in Section IV, and the paper is concluded in Section V.

II. Channel Model and Iterative Decoder

A. Channel model and capacity

The q-ary bit-measurement channel (QBMC) input alphabet consists of $q = 2^s$ symbols: $\mathcal{X} = \{0, 1, ..., q-1\}$. We refer to each symbol as a GF(q) field element, using the following standard polynomial representation [6]. A symbol $x \in \mathcal{X}$ is mapped to the polynomial $f_x(z) = \sum_{i=0}^{s-1} a_i z^i$, where the coefficients a_i are the binary representation of x. Arithmetic operations between the field elements are then defined modulo an irreducible polynomial of degree s over GF(2). For each input symbol x and a given j ($j = 0, 1, ..., s$), the output of the channel is a *set* of GF(q) symbols that are consistent with the partially observed symbol. That is, the output set contains 2^j consecutive symbols that have the same $s - j$ left bits as x in the binary representation. We denote the possible output sets by $\mathcal{M}_x^j$, and say that a *partial-erasure* event occurred if $j \geq 1$. The transition probabilities governing the QBMC are:

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

where ε_0 is the probability of no partial-erasure, and ε_j for $j = 1, ..., s$ are the partial-erasure probabilities.

Example 1. Assume that $q = 4$. The polynomial representation of the symbols in $\mathcal{X}$ is $\{0, 1, z, z+1\}$. If the input symbol is 0, the possible output sets are $\mathcal{M}_0^0 = \{0\}$ with probability

ε_0, $\mathcal{M}_0^1 = \{0,1\}$ with probability ε_1, and $\mathcal{M}_0^2 = \{0,1,2,3\}$ (i.e., full erasure) with probability ε_2.

We now move to derive the QBMC capacity.

Theorem 1. *The capacity of the QBMC channel defined by* (1) *is*

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

measured in q-ary symbols per channel use.

The proof of this theorem is based on standard capacity calculation and is omitted. As expected, the QBMC capacity reduces to the q-ary erasure channel (QEC) capacity if only ε_s is non-zero.

B. GF(q) LDPC codes and QBMC iterative-decoder

The error-correcting codes we consider for dealing with partial-erasure events are GF(q) LDPC codes [7]. These codes are defined by a sparse parity-check matrix with elements taken from GF(q), commonly visualized as a Tanner graph. This (bipartite) graph has *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 $\mathtt{c}$ is $\sum_{\mathtt{v}\in\mathcal{N}(\mathtt{c})} h_{\mathtt{c},\mathtt{v}} \cdot \mathtt{v} = 0$, where $\mathcal{N}(\mathtt{c})$ is the set of variable nodes adjacent to check node $\mathtt{c}$, and $h_{\mathtt{c},\mathtt{v}}$ are the labels on the edges connecting check node $\mathtt{c}$ to its neighbours. The calculations are performed using GF(q) arithmetic, where symbols are interpreted as GF(q) elements. In this work, we focus on *regular* LDPC codes, with check nodes of degree d_c and variable nodes of degree d_v. The code rate of a regular (d_v, d_c) ensemble is at least $1 - d_v/d_c$, with equality attained when the LDPC code parity-check matrix is of full rank [5].

GF(q) LDPC codes over the QBMC can be decoded using a message-passing decoder with messages consisting of symbol probabilities. Equivalently, we use the iterative decoder presented in [1] that extends the BEC iterative decoder [5] to partial erasures. The messages passed in this decoder, either *variable-to-check* (VTC) or *check-to-variable* (CTV) messages, are subsets of GF(q). 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 from $\mathtt{v}$ to $\mathtt{c}$ at iteration l. 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 (one of the sets $\mathcal{M}_x^j$ defined in Section II-A) to its adjacent check nodes. We denote these initial messages by $\mathrm{VTC}_{\mathtt{v}}^{(0)}$.

A CTV message at iteration $l \geq 1$ is a set containing all the possible symbol values of the target variable node that satisfy the check node parity-check equation given the incoming VTC messages at iteration $l-1$. We use the *sumset* operation [8] to calculate the CTV messages. The sumset of two sets $\mathcal{A}$ and $\mathcal{B}$ that contain GF(q) elements is defined as

$$\mathcal{A} + \mathcal{B} \triangleq \{a + b : a \in \mathcal{A}, b \in \mathcal{B}\}, \tag{3}$$

where the addition is performed using the GF(q) arithmetic. That is, $\mathcal{A}+\mathcal{B}$ is a set containing 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 (for characteristic-2 fields)

$$\mathrm{CTV}_{\mathtt{c}\to\mathtt{v}}^{(l)} = \sum_{\mathtt{v}'\in\{\mathcal{N}(\mathtt{c})\setminus\mathtt{v}\}} \left(\frac{h_{\mathtt{c},\mathtt{v}'}}{h_{\mathtt{c},\mathtt{v}}}\right) \cdot \mathrm{VTC}_{\mathtt{v}'\to\mathtt{c}}^{(l-1)}, \tag{4}$$

where the sum is sumset and the multiplications are performed element-wise. Once CTV messages are sent from all check nodes, an outgoing VTC message from variable node $\mathtt{v}$ to check node $\mathtt{c}$ is the *intersection* of the channel information set at $\mathtt{v}$ and its incoming CTV message sets:

$$\mathrm{VTC}_{\mathtt{v}\to\mathtt{c}}^{(l)} = \mathrm{VTC}_{\mathtt{v}}^{(0)} \bigcap \left\{ \bigcap_{\mathtt{c}'\in\{\mathcal{N}(\mathtt{v})\setminus\mathtt{c}\}} \mathrm{CTV}_{\mathtt{c}'\to\mathtt{v}}^{(l)} \right\}. \tag{5}$$

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 passed messages

In this section, we show that the VTC and CTV messages admit certain structural properties that facilitate decoding-performance analysis. Denote the additive group of GF(q) by $(\mathrm{GF}(q), +)$, and its subgroups by $\{\mathcal{H}_i\}_{i=1}^{t}$, where t is the number of subgroups. We start with two fundamental properties of the sumset and intersection operations between *cosets* of subgroups. Note that sums involving sets are understood as sumsets (see (3)).

Lemma 2. *Consider the cosets $\mathcal{H}_a + g_a$ and $\mathcal{H}_b + g_b$ for some field elements g_a and g_b. Then:*

$$(\mathcal{H}_a + g_a) + (\mathcal{H}_a + g_b) = (\mathcal{H}_a + \mathcal{H}_b) + (g_a + g_b). \tag{6}$$

In addition, if both cosets contain an element γ,

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

Proof. The right-hand side of (6) follows from the commutativity of (GF(q), +). As sumset of commutative subgroups results in a subgroup, the right-hand side of (6) is in fact a coset of the subgroup $\mathcal{H}_a+\mathcal{H}_b$. To prove (7), note that if $\gamma \in \mathcal{H}_a+g_a$ then $\mathcal{H}_a + g_a = \mathcal{H}_a + \gamma$. Similarly, $\mathcal{H}_b + g_b = \mathcal{H}_b + \gamma$. The coset $H_a+\gamma$ is actually a bijection $h_a \mapsto h_a+\gamma$ for $h_a \in \mathcal{H}_a$, where $H_b + \gamma$ is a bijection as well. As a result, (7) follows as an intersection of bijective functions. The intersection of subgroups is a subgroup, such that the right-hand side of (7) is a coset of the subgroup $\mathcal{H}_a \bigcap \mathcal{H}_b$. □

The properties derived in Lemma 2 imply that the sumset and intersection operations between cosets result in cosets. We now these properties to prove that messages passed in the decoding process are cosets. Let us define $\mathcal{M}_x^j(z)$ as the polynomials that correspond to the symbols in $\mathcal{M}_x^j$ (see Section II-A). In a similar manner, we define $\mathcal{H}_i(z)$ as the subgroup elements of $\mathcal{H}_i$ in polynomial representation.

Lemma 3. *Consider an instance of the QBMC iterative decoder. Then the VTC and CTV messages are cosets of subgroups of $(GF(q), +)$.*

Proof. The set $\mathcal{M}_0^j(z)$ for a particular j contains all polynomials of degree strictly less than j. As the sum of two such polynomials must have a degree strictly less than j, the elements of $\mathcal{M}_0^j(z)$ are closed under addition and thus $\mathcal{M}_0^j(z)$ is a *subgroup* of $(\mathrm{GF}(q), +)$. Moreover, the channel information set $\mathcal{M}_x^j$ is simply a translation of $\mathcal{M}_0^j$:

$$\mathcal{M}_x^j(z) = \mathcal{M}_0^j(z) + f_x(z), \tag{8}$$

where the addition is performed element-wise. This establishes channel-information sets as cosets of $\mathcal{M}_0^j(z)$.

Now assume the transmission of a codeword $\boldsymbol{x}$, where $x_{\mathtt{v}}$ is the codeword symbol corresponding to variable node $\mathtt{v}$ and $f_{x_{\mathtt{v}}}(z)$ is its polynomial representation. The CTV message from check node $\mathtt{c}$ to variable node $\mathtt{v}$ at iteration 1 is then (see (4))

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

where for a given $\mathtt{v}'$, $g_{\mathtt{v}'}(z)$ is a constant determined by the edge labels, $2^{j_{\mathtt{v}'}}$ is the channel-information set cardinality at $\mathtt{v}'$, and $f_{x_{\mathtt{v}'}}(z)$ is the correct codeword symbol at $\mathtt{v}'$. A set $g_{\mathtt{v}'}(z)\cdot\mathcal{M}_0^{j_{\mathtt{v}'}}(z)$ is a subgroup, where closure follows from the closure of $\mathcal{M}_0^{j_{\mathtt{v}'}}(z)$. Thus, (9) is a coset, using the first part of Lemma 2. Since $f_{x_{\mathtt{v}}}(z)$ belongs to this coset (recall that the channel may introduce partial erasures but no errors), (9) can be written as

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

which is interpreted as a coset of the subgroup obtained as the sumset of the subgroups incoming to node $\mathtt{v}$.

The VTC message at iteration 1 from $\mathtt{v}$ to $\mathtt{c}$ is the intersection between the channel information coset $\mathcal{M}_0^{j_{\mathtt{v}}}(z) + f_{x_{\mathtt{v}}}(z)$ and CTV messages of the form (10) (which were shown to be cosets). As $f_{x_{\mathtt{v}}}(z)$ belongs to this intersection, we obtain a coset of the form (using the second part of Lemma 2):

$$\left(\mathcal{M}_0^{j_{\mathtt{v}}}(z)\bigcap_{\mathcal{V}_j'}\sum_{\mathtt{v}'\in\mathcal{V}_j'} g_{\mathtt{v}'}(z)\cdot\mathcal{M}_0^{j_{\mathtt{v}'}}(z)\right) + f_{x_{\mathtt{v}}}(z), \qquad (11)$$

for a variable node set $\mathcal{V}_j'$ that depends on $\mathtt{c}$ only. Repeating the arguments above for the next decoding iterations, an invariant is maintained that the VTC and CTV messages are cosets of subgroups of $(\mathrm{GF}(q),+)$ at each decoding iteration. □

The following is an important outcome of Lemma 3.

Theorem 4. *Consider a fixed Tanner graph with given channel-information sets at variable nodes. The probability of decoding failure is independent of the transmitted codeword. Furthermore, assuming the transmission of the all-zero codeword, the possible messages are subgroups of* $(GF(q),+)$.

Proof. We formally prove the intuitive fact that decoding progress only depends on the *subgroups* exchanged in the messages, and not on which cosets of these subgroups are exchanged. Consider the CTV (resp. VTC) messages at iteration 1 calculated in (10) (resp. (11)). The sets $\mathcal{M}_0^{j_{\mathtt{v}}}$ and $g_{\mathtt{v}'}\cdot\mathcal{M}_0^{j_{\mathtt{v}'}}$ are independent of the actual transmitted codeword but rather depend on the *partial-erasure pattern*, i.e., on the cardinalities $2^{j_{\mathtt{v}}}$ (in addition to the edge labels that are a property of the Tanner graph). Therefore, the messages (10)-(11) can be considered as the result of the all-zero codeword transmission up to a translation by $f_{x_{\mathtt{v}}}(z)$.

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). Subgroups and their cosets have the same cardinality, thus the message-set cardinality on a certain edge is the same for all the codewords. As a consequence, the probability of decoding failure is independent of the transmitted codeword. Assuming that the all-zero codeword is transmitted, $f_{x_{\mathtt{v}}}(z)$ are all zero. In this case, the CTV (resp. VTC) messages (10) (resp. (11)) are sumsets (resp. intersections) of $(\mathrm{GF}(q),+)$ *subgroups*, which result in subgroups. □

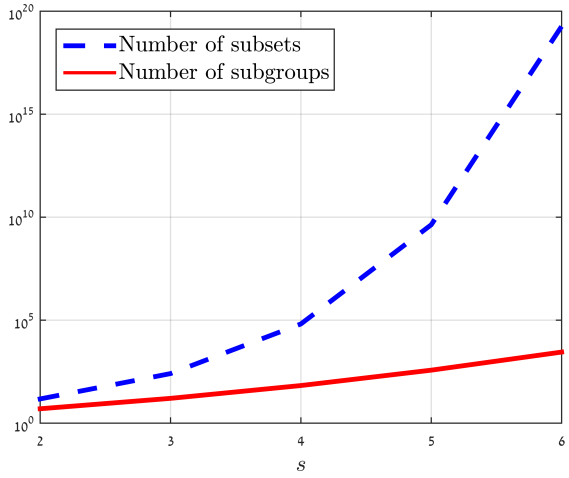

Fig. 1: The number of subgroups of $(\mathrm{GF}(q=2^s),+)$ compared to the number of subsets.

We remark that the possible subgroups transmitted as messages given the transmission of the all-zero codeword are not necessarily restricted to the channel-information subgroups $\mathcal{M}_0^j$. This is due to the edge labels that multiply VTC messages. To analyze the performance of the QBMC iterative decoder, we need to track the probabilities of the passed messages. The complexity of this analysis depends on the size of the space of possible messages.

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*

$$t=\sum_{j=0}^{s}\left(\frac{\prod_{i=1}^{j}\left(2^s-2^{i-1}\right)}{\prod_{i=1}^{j}\left(2^j-2^{i-1}\right)}\right), \qquad (12)$$

which is the number of subgroups of $(\mathrm{GF}(q=2^s),+)$.

Note that the number of subgroups of cardinality 2^j is the j^{th} summand in (12). The proof of theorem (5) is based on representing $(\mathrm{GF}(q=2^s),+)$ as an s-dimensional vector space over GF(2). The number of subgroups of order 2^j is then found as the number of subspaces of dimension 2^j (see e.g. [9] for the details). In Figure 1, the number of subgroups is plotted compared to the number of non-empty subsets of $(\mathrm{GF}(q),+)$ as a reference. This figure reveals the importance of the QBMC structure to the analysis feasibility, by which the number of subgroups is orders of magnitude smaller compared to the number of subsets of $(\mathrm{GF}(q),+)$. We remark that the actual number of subgroups passed in the decoding process is not necessarily t, and 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 only ε_0 and ε_s are non-zero) are $\{0\}$ and $\{0,1,...,q-1\}$.

IV. The QBMC Decoding Threshold Region

In the density evolution method [10], [11], the asymptotic (in terms of codeword length) probability of the passed messages at each decoding iteration is tracked, where the aim is to calculate the probability of decoding failure. Let us consider a

Tanner graph drawn uniformly at random out of graphs with variable-node degree d_v and check-node degree d_c. We assume a sufficiently large codeword length, such that the possible messages are statistically independent with high probability [10]. The all-zero codeword is transmitted (see Theorem 4), such that the possible messages are subgroups of $(\mathrm{GF}(q),+)$. For convenience, the subgroups $\{\mathcal{H}_i\}_{i=1}^{t}$ of $(\mathrm{GF}(q),+)$ are ordered by size, and lexicographically within each size. Recall that the number of subgroups t is given in (12).

Example 2. There are $t=5$ subgroups of $(\mathrm{GF}(q=4),+)$: $\mathcal{H}_1=\{0\}$, $\mathcal{H}_2=\{0,1\}$, $\mathcal{H}_3=\{0,2\}$, $\mathcal{H}_4=\{0,3\}$ and $\mathcal{H}_5=\{0,1,2,3\}$. An element h in $\mathcal{H}_i$ is interpreted as its polynomial representation $f_h(z)$.

In the case of binary LDPC codes, the edge labels of a Tanner graph are simply '1's. However, the edge labels in the GF(q) case are taken from the non-zero field elements. Thus, a GF(q) LDPC ensemble is characterized by *both* degree distributions and edge-label probability distribution, where we denote the latter distribution by $\mathbb{L}$. To obtain the QBMC density-evolution equations, we proceed as follows. Define $w_i^{(l)}$ (resp. $z_i^{(l)}$) as the probability that a CTV (resp. VTC) message at iteration l is $\mathcal{H}_i$. In addition, denote an ordered list containing incoming VTC (resp. CTV) message (subgroup) indices to a check (resp. variable) node by $\mathcal{S}_{\mathrm{VTC}}$ (resp. $\mathcal{S}_{\mathrm{CTV}}$). The elements in the lists are taken from $\{1,2,...,t\}$, where $|\mathcal{S}_{\mathrm{VTC}}|=d_c-1$ and $|\mathcal{S}_{\mathrm{CTV}}|=d_v-1$.

Example 3. Assume that $q=4$ (i.e., $t=5$ subgroups), $d_v=3$ and $d_c=6$. Then the possible realizations of $\mathcal{S}_{\mathrm{VTC}}$ are $[1,1,1,1,1],[1,1,1,1,2],\ldots,[5,5,5,5,5]$, and the possible realizations of $\mathcal{S}_{\mathrm{CTV}}$ are $[1,1],[1,2],\ldots,[5,5]$.

We define $P_i(\mathcal{H}_{m\in\mathcal{S}_{\mathrm{VTC}}},)$ as the probability of the CTV message $\mathcal{H}_i$ given the incoming VTC messages indexed in $\mathcal{S}_{\mathrm{VTC}}$ and the edge-label probability distribution $\mathbb{L}$. $I_i^j(\mathcal{H}_{m\in\mathcal{S}_{\mathrm{CTV}}})$ is an indicator function, which equals 1 if the intersection of the CTV messages indexed in $\mathcal{S}_{\mathrm{CTV}}$ and the channel-information set $\mathcal{M}_0^j$ results in $\mathcal{H}_i$. Otherwise, $I_i^j(\mathcal{H}_{m\in\mathcal{S}_{\mathrm{CTV}}})$ is 0 (note that the calculation of I_i^j is independent of the edge labels). The following density-evolution equations are obtained:

$$w_i^{(l)}=\sum_{\mathcal{S}_{\mathrm{VTC}}}\left(\prod_{m\in\mathcal{S}_{\mathrm{VTC}}}z_m^{(l-1)}\right)\cdot P_i\left(\mathcal{H}_{m\in\mathcal{S}_{\mathrm{VTC}}},\mathbb{L}\right), \quad (13)$$

$$z_i^{(l)}=\sum_{j=0}^{s}\varepsilon_j\sum_{\mathcal{S}_{\mathrm{CTV}}}\left(\prod_{m\in\mathcal{S}_{\mathrm{CTV}}}w_m^{(l)}\right)\cdot I_i^j\left(\mathcal{H}_{m\in\mathcal{S}_{\mathrm{CTV}}}\right). \quad (14)$$

The initial conditions of Equations (13)-(14) are determined by the transition probabilities in (1). That is, $z_1^{(0)}=\varepsilon_0$ and $z_i^{(0)}$ with i such that $\mathcal{H}_i$ equals $\mathcal{M}_0^j$ ($j\geq 1$) are initialized to ε_j. For example, if $q=4$, then $z_1^{(0)}=\varepsilon_0$, $z_2^{(0)}=\varepsilon_1$ and $z_5^{(0)}=\varepsilon_2$, where $z_3^{(0)}=z_4^{(0)}=0$. The asymptotic probability of decoding failure at iteration l, denoted $P_{\mathrm{error}}^{(l)}$, is the probability that a VTC message at iteration l is not $\{0\}$:

$$P_{\mathrm{error}}^{(l)}=\sum_{i=2}^{t}z_i^{(l)}=1-z_1^{(l)}. \quad (15)$$

The QBMC is characterized by multiple partial-erasure probabilities $\{\varepsilon_j\}_{j=1}^{s}$ rather than by a single erasure probability (as in the BEC). Thus, we define the *QBMC decoding threshold region* by extending the BEC decoding threshold [5]. First, define the following *QBMC* $\mathbb{L}$*-region* for given (d_v,d_c) pair and edge-label distribution $\mathbb{L}$:

$$\Omega_{\mathbb{L}}(d_v,d_c)=\left\{\varepsilon_1,\varepsilon_2,...,\varepsilon_s\in[0,1]^s:\lim_{l\to\infty}P_{\mathrm{error}}^{(l)}(\mathbb{L})=0\right\}. \quad (16)$$

The QBMC decoding threshold region is the union of the QBMC $\mathbb{L}$-regions over all possible choices of $\mathbb{L}$:

$$\Omega(d_v,d_c)=\bigcup_{\mathbb{L}}\Omega_{\mathbb{L}}(d_v,d_c). \quad (17)$$

That is, the QBMC decoding threshold region is an s-dimensional region that contains the partial-erasure probability values resulting asymptotically in successful iterative decoding for some choice of $\mathbb{L}$. If both the boundaries of $\Omega(d_v,d_c)$ and $\Omega_{\mathbb{L}}(d_v,d_c)$ contain the same certain point, we say that $\mathbb{L}$ is *optimal* with respect to this point.

A. Edge-label distribution and decoding performance

Let us assume that the edge labels are i.i.d. random variables, where $\ell_j\triangleq\Pr(\text{The edge label is } j)$ for $j=1,\ldots,q-1$ and $\mathbb{L}=\{\ell_j\}_{j=1}^{q-1}$. Our aim here is to demonstrate how choosing $\mathbb{L}$ wisely leads to an improvement in the asymptotic decoding performance. For this purpose, we investigate the density-evolution equations (13)-(14) when $q=4$ and $\varepsilon_2=0$ (no full erasures). In this case (assuming the all-zero codeword), the only possible partial-erasure VTC message is $\{0,1\}$, and a variable node remains partially erased if and only if all its incoming CTV messages are either $\{0,1\}$ or $\{0,1,2,3\}$. Denote the probabilities of these CTV messages at iteration l by α_l and β_l, respectively. In addition, denote by x_l the probability of the VTC message $\{0,1\}$ at iteration l.

Due to the closure of the $\{0,1\}$ subgroup elements, the sumset of $\{0,1\}$ with itself results in $\{0,1\}$. Thus, to obtain a CTV $\{0,1\}$ message, we need that at least one summand in (4) is $\{0,1\}$, and the rest are either $\{0,1\}$ or $\{0\}$. A summand of $\{0,1\}$ is obtained when the VTC message is $\{0,1\}$, and the incoming edge label from $\mathtt{v}'$ equals the outgoing edge label to $\mathtt{v}$. Overall the probability of the CTV message $\{0,1\}$ is given in the following, where the sum index r is the number of incoming $\{0,1\}$ VTC messages

$$\alpha_l=\sum_{r=1}^{d_c-1}\binom{d_c-1}{r}x_l^r(1-x_l)^{d_c-r-1}\left[\sum_{j=1}^{3}\ell_j^{r+1}\right], \quad (18)$$

and $\sum_{j=1}^{q-1}\ell_j^{r+1}$ ($r\in\{1,2,...,d_c-1\}$) is the probability that all edge labels of $\{0,1\}$ messages equal the outgoing edge label. For the CTV message $\{0,1,2,3\}$ (full erasure), at least two of the incoming VTC messages must be $\{0,1\}$, and at least two of those messages must have different edge labels. The probability of CTV message $\{0,1,2,3\}$ is thus

$$\beta_l=\sum_{r=2}^{d_c-1}\binom{d_c-1}{r}x_l^r(1-x_l)^{d_c-r-1}\left[1-\sum_{j=1}^{3}\ell_j^r\right]. \quad (19)$$

Our interest lies in the sum $\alpha_l+\beta_l$, which is required to calculate x_{l+1}. To simplify this sum, we use the following identity based on the binomial distribution's generating function for $\eta\in\mathbb{R}$

$$\sum_{r=0}^{d_c-1}\eta^r\binom{d_c-1}{r}x_l{}^r(1-x_l)^{d_c-r-1} \quad (20)$$
$$=(1-x_l+\eta x_l)^{d_c-1},$$

to obtain

$$\alpha_l + \beta_l = \tag{21}$$
$$1 + (1 - x_l)^{d_c - 1} - \sum_{j=1}^{3} (1 - \ell_j) \left(1 - x_l \cdot (1 - \ell_j)\right)^{d_c - 1}.$$

A variable node remains partially-erased at iteration $l+1$ if it was partially-erased initially (with probability ε_1), and its $d_v - 1$ incoming CTV messages are either $\{0, 1\}$ or $\{0, 1, 2, 3\}$. This leads to the following *single-letter* recurrence relation

$$x_{l+1} = \varepsilon_1 \cdot (\alpha_l + \beta_l)^{d_v - 1}. \tag{22}$$

If $\ell_1 = \ell_2 = 1/2, \ell_3 = 0$ (or symmetrically any two ℓ_j each equal $1/2$ with the third being 0), (22) becomes

$$x_{l+1} = \varepsilon_1 \left(1 - \left(1 - \frac{x_l}{2}\right)^{d_c - 1}\right)^{d_v - 1}. \tag{23}$$

We give the recurrence above for regular ensembles (fixed d_v, d_c), but it is readily extended to irregular ensembles as well. The outcome of the derivation (23) is that we obtain the same recurrence equation as the BEC/QEC density evolution, only with $x_l/2$ replacing x_l at the right-hand side. This is clearly optimal because it implies an ε_1 threshold that is *double* the BEC threshold for the same ensemble, and thus a capacity-achieving BEC ensemble will give a capacity-achieving QBMC ensemble according to (2) (for $s = 2$ and $\varepsilon_2 = 0$). At the other extreme, the worst choice of label distribution is $\ell_1 = 1, \ell_2 = \ell_3 = 0$ (binary codes), which gives the same threshold of the BEC without doubling[1]. It is an interesting fact that achieving optimality requires a label distribution that is *not* the uniform distribution over the non-zero elements of GF(4). Instead, to obtain optimal correction of QBMC partial erasures of cardinality 2, we need to choose the label distribution $\ell_1 = \ell_2 = 1/2, \ell_3 = 0$. We note that if cardinality 2 partial erasures is the only type of erasure the QBMC ever outputs, we can alternatively achieve optimality by using a binary capacity-achieving ensemble on the least significant bit (LSB) of the symbol, leaving the most significant bit (MSB) uncoded. But the advantage of q-ary ensembles with $\ell_1 = \ell_2 = 1/2, \ell_3 = 0$ is that in addition to the optimality for $\varepsilon_2 = 0$, the same code has good correction performance for infinitely many combinations of ε_1, ε_2.

In Figure 2, the boundary of the QBMC $\mathbb{L}$-region defined in (16) is plotted for the $\ell_1 = \ell_2 = 1/2, \ell_3 = 0$ edge-label distribution (dotted line) and for the uniform $\ell_1 = \ell_2 = \ell_3 = 1/3$ distribution (solid line), for the $(3, 6)$ LDPC code ensemble. The boundary of the QBMC capacity region is also plotted (dashed line) for reference. For the $\ell_1 = \ell_2 = 1/2, \ell_3 = 0$ distribution, the lower-right corner is $\varepsilon_1 = 0.858$, double the BEC threshold 0.429 as discussed above. At the upper-left corner ($\varepsilon_1 = 0$), both label distributions attain the same ε_2 threshold – identical to the standard BEC threshold for full erasures. While the $\ell_1 = \ell_2 = 1/2, \ell_3 = 0$ distribution is superior at the lower-right corner, Figure 2 reveals that there are values of $\varepsilon_2 > 0$ at which the uniform distribution has a higher ε_1 threshold. This hints that in general there is no single distribution $\mathbb{L}$ universally optimal for all combinations of $\{\varepsilon_j\}_{j=1}^{s}$.

[1]This implies that with binary codes 1-bit erasures are as "costly" as full q-ary symbol erasures.

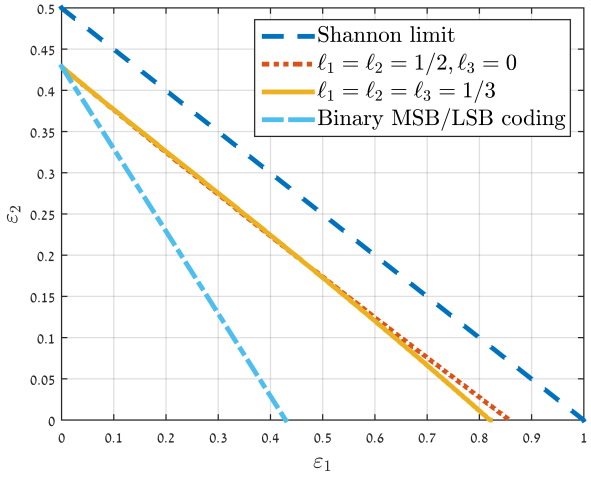

Fig. 2: The GF(4) QBMC $\mathbb{L}$-region boundaries of two edge-label distributions for the $(3, 6)$ LDPC code ensemble (design rate = $1/2$). The QBMC capacity region is also plotted for reference. The dash-dotted line refers to a naive independent binary coding of the MSB and LSB bits (each with the $(3, 6)$ LDPC code ensemble), which is significantly worse compared to the use of GF(4) LDPC codes.

V. Conclusion

This work offers a study of the performance of iterative decoding of GF(q) LDPC codes over the QBMC. The iterative decoder was shown to posses important structural properties that result in simplified analysis. In addition, it was demonstrated explicitly how the edge-label distribution affects decoding performance. Our work leaves interesting problems for future research, most immediately the joint optimization of degree and edge-label distributions.

Acknowledgement

This work was supported in part by the Israel Science Foundation and by the German-Israel Foundation.

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] 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.

[3] K. Haymaker and C. A. Kelley, "Structured bit-interleaved LDPC codes for MLC flash memory," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 5, pp. 870–879, May 2014.

[4] F. Zhang, H. D. Pfister, and A. Jiang, "LDPC codes for rank modulation in flash memories," in *2010 IEEE International Symposium on Information Theory*, June 2010, pp. 859–863.

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

[6] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*. Kluwer Academic Publishers, 1987.

[7] 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.

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

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

[10] 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.

[11] 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.