Estimation of the Decoding Threshold of LDPC Codes over the q-ary Partial Erasure Channel

Rami Cohen and Yuval Cassuto
Department of Electrical Engineering
Technion - Israel Institute of Technology
Technion City, Haifa 3200000, Israel
Email: rc@tx.technion.ac.il, ycassuto@ee.technion.ac.il

***Abstract*—In this paper, we discuss bounds and approximations for the decoding threshold of LDPC codes over the q-ary partial erasure channel (QPEC), introduced in [1]. The QPEC has a q-ary input, and its output is either one symbol or a set of $2 \leq M \leq q$ possible symbols. We show how an upper bound on the decoding threshold can be derived using a single-letter recurrence relation, when $M > q/2$. In addition, we discuss complexity issues in the calculation of the threshold, and provide two approximation models that lead to reasonable results with a fraction of the complexity required for the exact calculation.**

I. Introduction

Linear codes constructed from low density matrices, known as low-density parity-check (LDPC) codes [2], [3], offer low complexity in implementation, with good performance under iterative decoding [4]. These codes were shown to achieve performance close to the capacity for several important channels, using efficient decoding algorithms.

LDPC codes are part of several digital communication standards, such as 10GBase-T Ethernet and WiMax [5]. They have performance exceeding in many cases that of turbo codes. In particular, iterative decoding algorithms used in LDPC codes are usually easier to implement, and are also parallelizable in hardware.

In several works by Richardson et al. [6], [7], an extensive analysis of LDPC codes over binary memoryless symmetric (BMS) channels is provided. It is shown that in many cases, LDPC codes exhibit a threshold phenomenon. That is, when the noise parameter of the channel is below a certain threshold, an arbitrary small error probability can be achieved. This analysis was extended to q-ary LDPC codes, such as done in [8], [9].

In [1], a new channel model was introduced, named the q-ary partial erasure channel (QPEC). This channel has a q-ary input, where its output is known up to M possible symbols ($2 \leq M \leq q$). The q-ary erasure channel (QEC) is a special case of the QPEC when $M = q > 2$, and the BEC is a special case of the QPEC when $M = q = 2$. However, unlike the determination of the decoding threshold for the BEC/QEC, finding the threshold for the QPEC when $M < q$ involves non-trivial density evolution equations, as shown in [1].

Several bounds and approximation models were suggested in [1] for estimating the decoding threshold of LDPC codes used over the QPEC. In this paper, we offer a new upper bound on the decoding threshold, using a single-letter recurrence relation. We also provide two new approximation models for the density evolution equations of the QPEC, which provide in turn approximations of the decoding threshold.

This paper is structured as follows. We review the channel model for the QPEC and the density evolution equations for decoding LDPC codes over this channel in Section II. An upper bound on the decoding threshold for $M > q/2$ is derived in Section III. Complexity issues and approximation models for the density evolution equations are discussed in Section IV. Finally, conclusions are given in Section V.

II. Preliminaries

A. Channel model

A *partial erasure* in the *q-ary Partial Erasure Channel* (QPEC) model represents an event where a symbol is received with uncertainty. In contrary to the q-ary erasure channel (QEC), where an erasure event means that the output symbol can be any of q possible symbols, in the QPEC it is limited to be one of M ($2 \leq M \leq q$) symbols.

The channel is defined as follows. Let X be the transmitted symbol taken from the alphabet $\mathcal{X} = \{0, 1, ..., q-1\}$. We will assume that q is a prime or a prime power, such that the symbols in $\mathcal{X}$ can be considered as the elements of the finite field GF(q). For each $x \in \mathcal{X}$, define the set $\left\{?_x^{(i)}\right\}_{i=1}^{i_{\max}}$, $i_{\max} = \begin{pmatrix} q-1 \\ M-1 \end{pmatrix}$, where each *super-symbol* $?_x^{(i)}$ ($?_x^{(i)} \neq ?_x^{(j)}$ for $i \neq j$) is a set of size M that contains the symbol x and $M-1$ other symbols, taken from $\mathcal{X} \setminus \{x\}$.

Let Y be the received symbol with the output alphabet $\mathcal{Y} = \left\{\mathcal{X} \bigcup_{x=0}^{q-1} \left\{?_x^{(i)}\right\}_{i=1}^{i_{\max}}\right\}$. The transition probabilities governing the QPEC are as follows:

$$\Pr\left(Y = y \mid X = x\right) = \begin{cases} 1-\varepsilon, & y = x \\ \varepsilon / i_{\max}, & y = ?_x^{(i)} \end{cases} \quad (1)$$

for $i = 1, 2, ..., i_{\max}$, where $0 \leq \varepsilon \leq 1$ is the (partial) erasure probability.

As an example, assume that $q = 4, M = 2$, and the symbol 0 was transmitted. Then we have $?_0^{(1)} = \{0, 1\}, ?_0^{(2)} = \{0, 2\}$ and $?_0^{(3)} = \{0, 3\}$, where each is received with probability $\varepsilon/3$ and 0 is received with probability $1 - \varepsilon$.

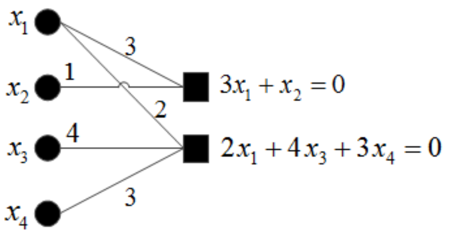


Fig. 1: Example for a Tanner graph (over GF(5)). Circles denote variable nodes, and squares denote check nodes.

B. Decoding GF(q) LDPC codes over the QPEC

A GF(q) $[n,k]$ LDPC code is defined in a similar way to its binary counterpart, by a sparse parity-check matrix, or equivalently by a Tanner graph [10]. This graph is bipartite, with n variable (left) nodes, which correspond to symbols of the codeword, and $n-k$ check (right) nodes, which correspond to parity-check equations. The codeword symbols and the labels on the graph edges are taken from GF(q).

In the graph, each check node c_j is connected, by edges, to variable nodes $v_i, i \in N(j)$, where $N(j)$ denotes the set of nodes adjacent to node j. The parity-check equation induced by c_j is $\sum\limits_{i \in N(j)} h_{ij} v_i = 0$, where h_{ij} is the label on the edge connecting variable node i to check node j. Note that the calculations are carried over GF(q). An example of a Tanner graph is given in Figure 1.

A message-passing decoder for q-ary LDPC codes over the QPEC was proposed in [1]. The beliefs exchanged in the decoding process are *sets of symbols*, rather than probabilities. There are two types of messages: *check to variable* (CTV) messages and *variable to check* (VTC) messages. Each outgoing message from a variable (check) node to a check (variable) node depends on all its incoming message, except for the incoming message originated from the target node.

At iteration $l = 0$, the channel information is sent from variable to check nodes: partially-erased nodes send sets of size M, while non-erased ones send sets of size 1 (in both cases, the messages contain the correct symbol). In the subsequent iterations, a CTV message from a check node contains all possible assignments of the target variable node given the contents of the incoming VTC messages, such that the check-node associated parity-check equation is satisfied. A VTC message from a variable node is simply the intersection of the channel information and the incoming CTV messages to the variable node.

C. Density evolution equations

For density evolution analysis of the QPEC, we introduce the notion of *sumset*. Assume that we have $i-1$ subsets of GF(q), $\{S_j\}_{j=1}^{i-1}$. The sumset of these subsets, denoted $\sum\limits_{j=1}^{i-1} S_j$, is defined in the following way:

$$\sum_{j=1}^{i-1} S_j \triangleq \left\{ \sum_{j=1}^{i-1} s_j : s_j \in S_j \right\}. \tag{2}$$

That is, the sumset of the subsets $\{S_j\}_{j=1}^{i-1}$ is the set of all sums (using GF(q) arithmetic) of elements taken from these subsets. There are $\prod\limits_{j=1}^{i-1} |S_j|$ sums within the sumset, each leading to an element of GF(q). Clearly, these elements are not necessarily distinct.

Define the probability vector $\mathbf{w}^{(l)}$, where $w_m^{(l)}$ ($m = 1, 2, ..., q$) denotes the probability that a CTV message at iteration l is of size m. The probability vector $\mathbf{z}^{(l)}$ is defined for VTC messages in a similar manner. In addition, define the polynomials (degree distributions) $\lambda(x) = \sum\limits_i \lambda_i x^{i-1}$ and $\rho(x) = \sum\limits_i \rho_i x^{i-1}$, where λ_i (ρ_i) denotes the fraction of edges connected to a variable node (check node) of degree i [4]. The density evolution equations for the QPEC are [1]:

$$w_m^{(l)} = \sum_i \rho_i \sum_{\substack{\{|S_j|\}_{j=1}^{i-1} : \\ |S_j| \le M}} \left(\prod_{j=1}^{i-1} z_{|S_j|}^{(l-1)} \right) \cdot P_m \left(\{|S_j|\}_{j=1}^{i-1} \right) \tag{3}$$

$$\begin{aligned} z_m^{(l)} &= \delta[m-1] \cdot (1-\varepsilon) \\ &+ \varepsilon \sum_i \lambda_i \sum_{\substack{\{|S_j|\}_{j=1}^{i-1} : \\ |S_j| \le q}} \left(\prod_{j=1}^{i-1} w_{|S_j|}^{(l)} \right) \cdot Q_m \left(\left\{ \{|S_j|\}_{j=1}^{i-1}, M \right\} \right) \end{aligned} \tag{4}$$

where $P_m\left(\{|S_j|\}_{j=1}^{i-1}\right)$ denotes the probability that the sumset size of random $i-1$ sets (taken from GF(q)) with sizes $\{|S_j|\}_{j=1}^{i-1}$ equals m, and $Q_m\left(\left\{\{|S_j|\}_{j=1}^{i-1}, M\right\}\right)$ denotes the probability that the intersection of i random sets (taken from GF(q)) with sizes $\left\{\{|S_j|\}_{j=1}^{i-1}, M\right\}$ is of size m. The additional set of size M corresponds to the channel information in case of partial erasure. $\delta[m]$ denotes the discrete Dirac delta function. Note that for $m > M$, $z_m^{(l)} = 0$ (for all l), since the size of the intersection between sets with sizes $\left\{\{|S_j|\}_{j=1}^{i-1}, M\right\}$ is at most M.

An exact expression for Q_m was derived in [1]. However, an exact expression for P_m is unknown and is likely difficult to find [11]. Several approximation models and bounds for P_m were suggested in [1], which led to approximations and bounds for the decoding threshold of GF(q) LDPC codes used over the QPEC. In the following, we derive an additional upper bound on the decoding threshold when $M > q/2$. In addition, we provide two new approximations of Equation (3).

III. Upper Bound on the Decoding Threshold

The decoding threshold for LDPC codes over the QPEC is defined as the maximal allowed erasure probability such that $\lim\limits_{l \to \infty} \sum\limits_{i=2}^{M} z_i^{(l)} = 0$. This threshold will be denoted by ε_{th}. In [1], both lower and upper bounds on ε_{th} were obtained. However, they require the evaluation of the density evolution equations (3) and (4), which involve $M+q$ variables (M for $\mathbf{z}^{(l)}$ and q for $\mathbf{w}^{(l)}$). In this part, we obtain an upper bound for the case

$M > q/2$, using a *single-letter* recurrence relation, which is *independent* of both P_m and Q_m that appear in Equations (3) and (4).

A sufficient condition for an outgoing CTV message to be of size q is the *q-condition* [1], meaning that there is at least one pair of incoming VTC messages whose sum of sizes exceeds q (this can occur only when $M > q/2$). Therefore, $w_q^{(l)}$ is bounded from below by the probability that at least two incoming messages are of size M:

$$w_q^{(l)} \geq \sum_i \rho_i \sum_{j=2}^{i-1} \binom{i-1}{j} \left(z_M^{(l-1)}\right)^j \left(1 - z_M^{(l-1)}\right)^{i-1-j} \tag{5}$$
$$= 1 - \rho\left(1 - z_M^{(l-1)}\right) - z_M^{(l-1)} \rho'\left(1 - z_M^{(l-1)}\right).$$

Recall that $z_M^{(l-1)}$ is the probability that the size of a VTC message at iteration $l-1$ is of size M. A sufficient condition for this to happen is that a variable node is a partial erasure, and all its incoming CTV messages are of size q. Therefore,

$$z_M^{(l)} \geq \varepsilon \sum_i \lambda_i \left(w_q^{(l)}\right)^{i-1} = \varepsilon \lambda\left(w_q^{(l)}\right). \tag{6}$$

Combining (5) and (6), we get:

$$z_M^{(l)} \geq \varepsilon \lambda\left(1 - \rho\left(1 - z_M^{(l-1)}\right) - z_M^{(l-1)} \rho'\left(1 - z_M^{(l-1)}\right)\right), \tag{7}$$

with the initial condition $z_M^{(0)} = \varepsilon$. Note that we have used the fact that $\lambda(x)$ is an increasing function of x. The inequality in (7) applies to any $M > q/2$, for all q (which is prime or prime power), and it depends solely on the degree distributions $\lambda(x)$ and $\rho(x)$.

In the rest of this section, we will see how this inequality can be used for deriving an upper bound on the decoding threshold for the QPEC when $M > q/2$. Define $f(\varepsilon, x) = \varepsilon\lambda(1 - \rho(1-x) - x\rho'(1-x))$ (which is the right-hand side of the inequality (7), with $z_M^{(l-1)}$ replaced by x).

Lemma 1. *$f(\varepsilon, x)$ is an increasing function of both ε and x, for $\varepsilon, x \in [0,1]$.*

Proof: Taking the partial derivatives of $f(\varepsilon, x)$ with respect to ε and x, we get:

$$\frac{\partial f}{\partial \varepsilon} = \lambda(1 - \rho(1-x) - x\rho'(1-x)) \tag{8}$$

$$\frac{\partial f}{\partial x} = \varepsilon x \lambda'(1 - \rho(1-x) - x\rho'(1-x))\rho''(1-x). \tag{9}$$

$\rho(x), \lambda(x)$ and their derivatives are power series of x with non-negative coefficients, and they are non-negative for non-negative arguments. In particular, $\rho''(1-x) \geq 0$ since $0 \leq 1-x \leq 1$. Therefore, it is sufficient to prove that $g(x) = \rho(1-x) + x\rho'(1-x) \leq 1$ for establishing the non-negativity of the partial derivatives (8) and (9).

This is proved in the following manner. The derivative of $g(x)$ in the interval $(0,1)$ satisfies $g'(x) = -x\rho''(1-x) < 0$, meaning that $g(x)$ is a decreasing function of x. In particular, $g(x) \leq g(0) = \rho(1) = 1$, as needed. ∎

Lemma 2. *For a fixed ε, define $h_\varepsilon(x) = f(\varepsilon, x)$, and consider the i^{th} composition of $h_\varepsilon(x)$ with itself, denoted $h_\varepsilon^i(x)$. Then:*

$$z_M^{(l)} \geq h_\varepsilon^l\left(z_M^{(0)}\right), \quad l \geq 1. \tag{10}$$

Proof: $h_\varepsilon(x)$ is an increasing function of x (Lemma 1). In addition, $z_M^{(l)} \geq h_\varepsilon\left(z_M^{(l-1)}\right)$ according to (7). Thus,

$$h_\varepsilon\left(z_M^{(l-1)}\right) \geq h_\varepsilon\left(h_\varepsilon\left(z_M^{(l-2)}\right)\right), \quad l \geq 2. \tag{11}$$

Repeated application of the monotonicity property to the right-hand side of (11) leads to the inequality $h_\varepsilon\left(z_M^{(l-1)}\right) \geq h_\varepsilon^l\left(z_M^{(0)}\right)$, proving the lemma. ∎

Lemma 3. *The following threshold is well-defined:*

$$\varepsilon^* = \sup\left\{\varepsilon \in [0,1] : \lim_{l\to\infty} h_\varepsilon^l\left(z_M^{(0)}\right) = 0\right\}. \tag{12}$$

Proof: $h_\varepsilon^l\left(z_M^{(0)}\right)$ converges in the interval $[0,1]$ and is an increasing function of ε. This can be proved using Lemma 1 and similar arguments to those used in Section 3.10 of [4]. In addition, $h_{\varepsilon=0}^l\left(z_M^{(0)}\right) = 0$. Therefore, the threshold in (12) is well-defined. ∎

Theorem 4. *For a QPEC with $M > q/2$, $\varepsilon_{\text{th}} \leq \varepsilon^*$.*

Proof: $z_M^{(l)}$ is bounded from below by a strictly positive value for all l when $\varepsilon > \varepsilon^*$, as a result of Lemma 2 and Lemma 3. This implies that the probability of decoding error is non-zero, meaning that the decoding threshold ε_{th} cannot exceed ε^*. ∎

An additional upper bound on ε that depends on the average variable node degree and the average check node degree is given in the following theorem.

Theorem 5. *Define a_L (a_R) as the average variable (check) node degree. Then, for a QPEC with $M > q/2$:*

$$\varepsilon_{\text{th}} \leq 2\frac{a_L}{a_R}\left(1 - \left(1 - 2\frac{a_L}{a_R}\right)^{a_R}\right). \tag{13}$$

Proof: This bound is obtained by integrating both sides of (7) from 0 to ε. The details are similar to those appearing in the proof of Theorem 1 in [12] (where the BEC is considered) and are omitted. Note that this bound is non-trivial only when $\frac{a_L}{a_R} < \frac{1}{2}$. ∎

The decoding threshold is a monotone non-increasing function of M (for a given q) [1]. Therefore, the upper bounds of the last two theorems become tighter as M approaches $\left\lfloor \frac{q}{2} \right\rfloor + 1$.

IV. Evaluation of P_m

A. Complexity considerations

$P_m = P_m\left(\{|S_j|\}_{j=1}^{i-1}\right)$ in Equation (3) can be calculated exactly in a direct manner by averaging over the sumset sizes of all possible assignments of elements from GF(q) to the sets $\{S_j\}_{j=1}^{i-1}$, given their sizes $\{|S_j|\}_{j=1}^{i-1}$. Note that it can be assumed that $0 \in S_j$ for $j = 1, 2, ..., i-1$ due to the all-zero codeword assumption [1].

As an example, assume that $q = 4$ (that is, we work with GF(4)), and that we have $K = 2$ sets with sizes $|S_1| = |S_2| = 2$. In this case, S_1 and S_2 can each be one of the sets $\{0,1\},\{0,2\},\{0,3\}$. Consider the realization $S_1 = \{0,1\}, S_2 = \{0,2\}$. The resulting sumset is $S_1+S_2 = \{0+0,0+2,1+0,1+2\} = \{0,2,1,3\}$, leading to a sumset of size 4. On the other hand, the realization $S_1 = S_2 = \{0,1\}$ results in the sumset $S_1+S_2 = \{0+0,0+1,1+0,1+1\} = \{0,1\}$, which is of size 2. Running over all $\begin{pmatrix} 3 \\ 1 \end{pmatrix}^2 = 9$ possible realizations of the sumset S_1+S_2, we get 3 realizations that result in a sumset of size 2 and 6 realizations that result in a sumset of size 4. Therefore, $P_1 = 0, P_2 = 1/3, P_3 = 0$ and $P_4 = 2/3$.

Extending this to the general case, for given q, M and check-node degree i, an averaging over $\left(\sum_{j=1}^{M}\begin{pmatrix} q-1 \\ j-1 \end{pmatrix}\right)^{i-1}$ realizations of the sets $\{S_j\}_{j=1}^{i-1}$ is required, making it infeasible as q, M or i increase. The following lemma shows how the number of required realization can be reduced, and it is a simple result of the commutativity of the '+' operation in a finite field.

Lemma 6. *Assume a fixed set of sizes $\{|S_j|\}_{j=1}^{i-1}$. Then, for any permutation $\pi : \{1,2,..,i-1\} \to \{1,2,..,i-1\}$, P_m is invariant to π, that is:*

$$P_m\left(\{|S_j|\}_{j=1}^{i-1}\right) = P_m\left(\left\{\left|S_{\pi(j)}\right|\right\}_{j=1}^{i-1}\right). \tag{14}$$

The meaning of Lemma 6 is that instead of averaging over the realizations of M^{i-1} possible sets of sizes for each check-node degree i in Equation (3), it is sufficient to consider only the realizations of $\begin{pmatrix} i+M-2 \\ i-1 \end{pmatrix}$ sets (which is the number of *multisets* of cardinality $i-1$ taken from a set of cardinality M). For further reducing the number of needed realizations, the q-condition (see Section III), which is effective only when $M > q/2$, can be taken into account as well. For sets of sizes that satisfy this condition, we simply have that $P_m = \delta[m-q]$, with no need for averaging over the possible realizations.

B. Approximate density evolution equations

According to the definition of the QPEC, the initial probability vector $\mathbf{z}^{(0)}$ is non-zero only for $m = 1$ and $m = M$. In the computation of the density evolution equations, it can be seen experimentally that $\mathbf{z}^{(l)}$ remains approximately concentrated in $m = 1$ and $m = M$ for $l > 0$ as well. An example is given in Figure 2. The calculation of $\mathbf{w}^{(l)}$ from Equation (3) requires the evaluation of $\prod_{j=1}^{i-1} z_{|S_j|}^{(l-1)}$, which we name the *z-factor*, for all possible sets of sizes $\{|S_j|\}_{j=1}^{i-1}, |S_j| \le M$. Given that the main contribution to this factor is due to $z_1^{(l-1)}$ and $z_M^{(l-1)}$, we suggest the following two approximation models.

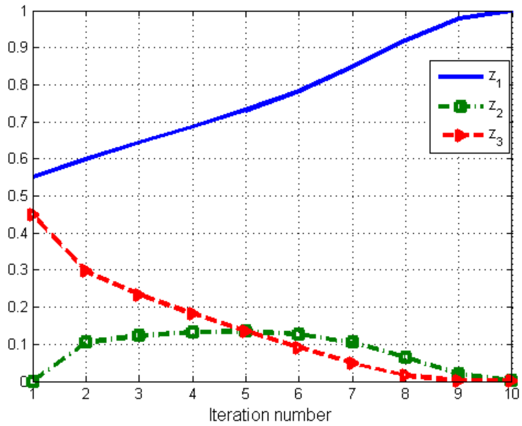


Fig. 2: Density evolution for $q = 4, M = 3, \varepsilon = 0.45$.

1) Model A: In this approximation model, the z-factor is approximated as zero if there exists at least one $|S_j|$ such that $|S_j| \ne 1, M$. Therefore, P_m needs to be calculated only for sets of sizes that contain $1, M$ or both, leading to a significant reduction in complexity.

Note that for $M > q/2$, P_m is easy to calculate for sets of sizes that result in a non-zero z-factor according to Model A. In this case, we get:

$$P_m = \begin{cases} \delta[m-1], & |S_j| = 1 \text{ for all } j \\ \delta[m-q], & \text{if the } q\text{-condition holds} \\ \delta[m-M], & \text{otherwise} \end{cases} \tag{15}$$

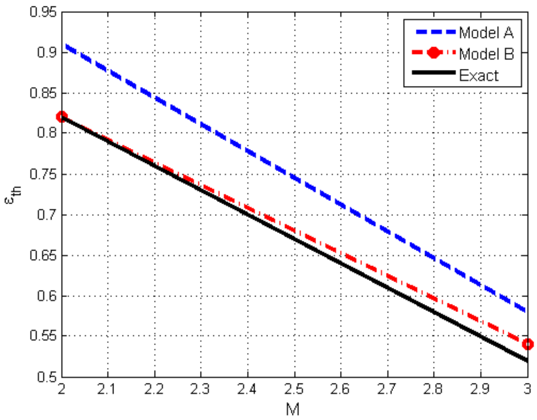
where $P_m = \delta[m-M]$ corresponds to sets of sizes in which one set is of size M and the remaining ones are of size 1. According to Equation (15), *no realizations* of $\{S_j\}_{j=1}^{i-1}$ are needed when $M > q/2$.

2) Model B: In this more accurate model, the z-factor is approximated as zero if there exist at least two $|S_j|$ such that $|S_j| \ne 1, M$. This model requires a higher complexity compared to Model A, since P_m needs to be calculated for additional realizations of sets for which the z-factor is non-zero.

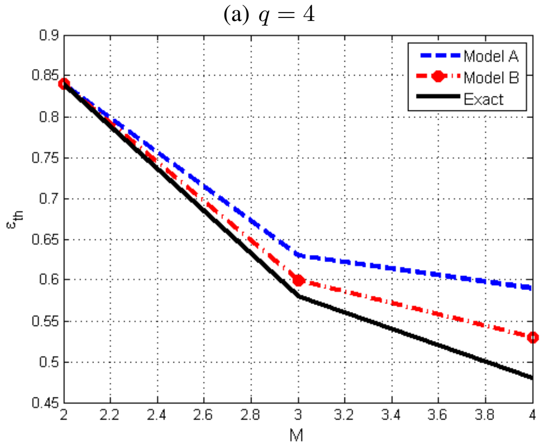
C. Calculation of the decoding threshold

The decoding threshold for the case $M = q$ can be calculated exactly using the density evolution equation of the BEC [1]. This threshold equals 0.429 for a $(3,6)$-regular LDPC code [4], [1], and it serves as a lower bound on the decoding threshold for $2 \le M < q$. The upper bound on the threshold for $M > q/2$ according to Theorem 4 is 0.719, and it is tighter than the upper bound of (13) which equals 1.

The decoding threshold was calculated exactly using the density evolution equations (3) and (4) for $q = 4$ and $q = 5$, for a $(3,6)$-regular LDPC code, where P_m was calculated efficiently according to the results of Section IV-A. In Figure 3, the exact threshold is compared to the threshold obtained using the approximate density evolution equations according to Models A and B. As expected, Model B provides a better approximation of the threshold compared to Model A.



(a) $q = 4$



(b) $q = 5$

Fig. 3: The decoding threshold for a (3,6)-regular LDPC code and its approximations.

The reduction in complexity when using the models is significant especially when $M > q/2$, since many of the sets of sizes for which the z-factor is not approximated as zero are likely to satisfy the q-condition. In Figure 4, the number of required realizations for the evaluation of P_m using the exact density evolution equations is compared to the number of realizations required when the models are used. This number is given for several values of q, summed over all $M > q/2$.

As shown in Figure 4, the use of the approximation models leads to a very significant reduction in the number of required realizations. Even for small values of q, a reduction of several orders of magnitude is clearly seen. Note that according to Figures 3 and 4, Model B provides approximate thresholds that are within 10% of the correct ones, making this model especially attractive.

V. Conclusions

In this paper, we provided upper bounds on the decoding threshold of GF(q) LDPC codes over the QPEC, for the case $M > q/2$. These bounds were derived using a single-letter recurrence relation, which can be a design tool used toward finding degree distributions that approach the Shannon capacity of the QPEC. This is a part of our ongoing research.

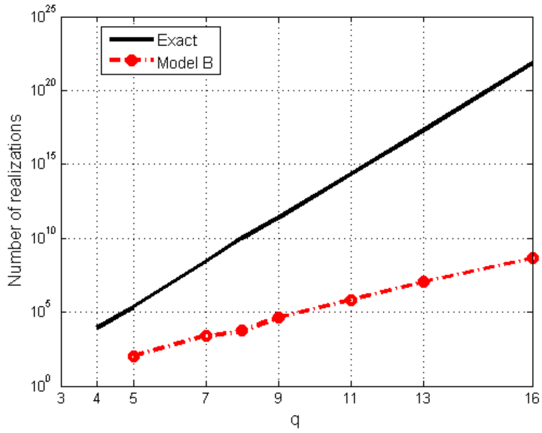


Fig. 4: The number of realizations required for evaluating P_m for $M > q/2$. This number is zero for all q in the case of Model A.

In addition, we provided approximation models for the calculation of the density evolution equations of the QPEC, leading to approximate decoding thresholds. These models provide reasonable estimates of the thresholds, for a fraction of the complexity required for the exact calculation of the density evolution equations.

VI. Acknowledgement

This work was supported in part by an EU CIG grant, by the Israel Ministry of Science and Technology, and by a Viterbi faculty fellowship.

References

[1] R. Cohen and Y. Cassuto, "LDPC codes for partial-erasure channels in multi-level memories," *ISIT 2014 (accepted)*, available online at http://arxiv.org/abs/1401.4799.

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

[3] ——, *Low-Density Parity Check Codes*. MIT Press, 1963.

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

[5] IEEE Standards Association. [Online]. Available: http://standards.ieee.org.

[6] 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.

[7] T. Richardson, A. Shokrollahi, and R. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 619–637, 2001.

[8] 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.

[9] 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.

[10] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inform. Theory* , vol. IT-27, pp. 533–547, 1981.

[11] E. Croot and V. F. Lev, "Open problems in additive combinatorics," Department of Mathematics, Georgia Institute of Technology, Tech. Rep., 2011.

[12] A. Shokrollahi, "New sequences of linear time erasure codes approaching the channel capacity," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, ser. Lecture Notes in Computer Science, M. Fossorier, H. Imai, S. Lin, and A. Poli, Eds. Springer Berlin Heidelberg, 1999, vol. 1719, pp. 65–76.