Weight Distribution of Non-Binary LDPC Codes

Iryna Andriyanova
EPFL, School of Communications &
Computer Sciences
1015 Lausanne, Switzerland
iryna.andriyanova@epfl.ch

Vishwambhar Rathi
EPFL, School of Communications &
Computer Sciences
1015 Lausanne, Switzerland
vishwambhar.rathi@epfl.ch

Jean-Pierre Tillich
Equipe-Projet SECRET
INRIA Roquencourt
France
jean-pierre.tillich@inria.fr

Abstract— **This paper is the first part of an investigation if the capacity of a binary-input binary-output memoryless symmetric channel under ML decoding can be achieved asymptotically by using non-binary LDPC codes. We consider (l,r)-regular LDPC codes both over finite fields and over the general linear group and compute asymptotic binary weight distributions for these ensembles in the limit of large blocklength and of large alphabet size. A surprising fact, the average binary weight distributions that we obtain do not tend to the binomial one for values of normalized binary weights ω smaller than $1-2^{-1/r}$. However, it does not mean that non-binary codes do not achieve the capacity asymptotically, but rather that there exists some exponentially small fraction of codes in the ensemble, which contains an exponentially large number of codewords of poor weight. The justification of this fact is beyond the scope of this paper and will be given in the extended version [1].**

I. Introduction

An important issue in coding theory is whether it is possible to achieve the capacity of a discrete memoryless symmetric channel (DMS) by using non-binary sparse-graph codes. If it were the case, one could probably design non-binary sparse-graph codes outperforming the binary ones from the point of view of the performance-complexity tradeoff. A common belief is that this might be true, and that by increasing the alphabet size of given code ensembles one comes closer to the channel capacity.

LDPC codes over non-binary alphabets have already been considered by Gallager in his PhD thesis [2]. In last years, there was a number of investigation of non-binary sparse-graph codes under iterative decoding, and an improvement of iterative decoding performances with the alphabet size has been observed both for turbo-codes [3]–[6] and for Low-Density Parity-Check (LDPC) codes [7]–[10]. This improvement is particularly apparent in the case of 2-regular LDPC codes [8]. It was also put forward in [10], that unlike in the binary case, where large degrees are needed to approach capacity, there are very good degree distributions for LDPC codes for large alphabet sizes, in the sense that all variable nodes have small degree and there is a very large fraction of variable nodes of degree 2. It is worthwhile to note however, that the code performances under iterative decoding do not always improve when one moves to a larger alphabet. Actually, the investigation performed for LDPC codes in [11] and for TLDPC codes in [12] on the binary erasure channel strongly suggests that for a given degree distribution, the iterative decoding threshold sustained by the code ensemble is a unimodal function of the alphabet size : it either always decreases with the alphabet size or increases up to a certain alphabet size and decreases afterwards.

What concerns the maximum likelihood (ML) decoding, the asymptotic error performance of regular non-binary coset LDPC ensembles has been derived in [13]. The coset mechanism was needed to satisfy a symmetry assumption attributed to the bounding technique [2] used. In [14] authors have obtained the average weight distribution of regular LDPC ensembles defined over the cyclic group of integers where the group operation is performed modulo an integer. It is also worth to mention a recent work of Hof et al [15], where the authors derive a new Gallager-like upper bound on the decoding error probability of non-binary linear codes under ML decoding, assuming transmission over DMS channels.

In this paper we consider non-binary (l,r)-regular LDPC codes, over finite fields and over the general linear group, and compute their asymptotic binary weight distributions in the limit of large blocklength and of large alphabet size. This weight distribution has also been derived very recently in [16], but without giving the quite intriguing asymptotic behavior for large alphabet size that we have found here. In order to present our main result, let us bring in the following quantities.

Definition 1: Denote by $N_b(G,nm\omega)$ the average number of codewords of binary weight $nm\omega$ of a code G of length n over GF_2^m chosen at random along either of the two models described in Section II. Define the growth rate by $\beta_m(\omega) \triangleq \lim_{n\to\infty} \frac{\log(\mathbb{E}(N_b(G,nm\omega)))}{nm}$ and its asymptotic expression by $\beta(\omega) \triangleq \lim_{m\to\infty} \beta_m(\omega)$.
We then have

Theorem 1.1:

$$\beta(\omega) = \begin{cases} -\omega\log(2^{1/\mathrm{r}}-1), & 0 \le \omega < 1-2^{-1/\mathrm{r}}, \\ h(\omega)-\frac{1}{\mathrm{r}}, & 1-2^{-1/\mathrm{r}} \le \omega \le 1. \end{cases}$$

II. Preliminaries

We consider regular non-binary LDPC ensembles, assuming that the alphabet size is a power of 2. Therefore, the components of a codeword are elements of the binary vector space of some dimension m denoted by GF_2^m. Non-binary ensembles are defined in the similar way as in the binary case, with the help of an ensemble of bipartite graphs $\mathbb{G}(n,l,r)$ (see [17] for definition). In this notation, l and r represent respective left and right degrees and n is the blocklength. Right nodes of a bipartite graph represent parity-check equations and left nodes - variables, participating in the equations. To each edge of the graph we assign a bijective linear mapping $f : \mathrm{GF}_2^m \mapsto \mathrm{GF}_2^m$. We perform the computation for two classes of regular non-binary LDPC codes: ensembles over finite fields and ensembles over the general linear group. The ensemble over the general linear group is denoted by $\mathrm{EGL}\,(n,l,r,m)$ and its mappings are chosen uniformly at random from the group of linear bijective mappings. Thus, the set of mappings is the general linear group GL_2^m of all the $m \times m$ invertible matrices. The ensemble over finite fields is denoted by $\mathrm{EGF}\,(n,l,r,m)$, and its mappings are of the form $f(x) = ax$, where $a \in \mathrm{GF}^*(2^m)$, the multiplicative group of $\mathrm{GF}(2^m)$. Therefore, the number of possible mappings in this case is $2^m - 1$. In what follows, we perform computations for both ensembles in parallel as they are very similar.

III. Expectation of the Weight Distribution

Let us begin by deriving the average weight distribution of the ensemble $\mathrm{EGL}\,(n,\mathtt{l},\mathtt{r},m)$.

Lemma 3.1 (Average Weight Distribution of EGL$\,(n,\mathtt{l},\mathtt{r},m)$): For $\mathrm{EGL}(n,\mathtt{l},\mathtt{r},m)$, the average weight distribution is

$$\mathbb{E}[N(G,n\omega)] = \frac{\binom{n}{n\omega}(2^m-1)^{n\omega}}{\binom{n\mathtt{l}}{n\mathtt{l}\omega}|\,\mathrm{GL}_2^m\,|^{n\mathtt{l}\omega}} \mathrm{coef}\left(p_m(y)^{\frac{n\mathtt{l}}{\mathtt{r}}}, y^{n\mathtt{l}\omega}\right), \quad (1)$$

where

$$p_m(y) = \frac{1}{2^m}\left[(1+|\,\mathrm{GL}_2^m\,|y)^{\mathtt{r}} + \left(1 - \frac{|\,\mathrm{GL}_2^m\,|y}{2^m-1}\right)^{\mathtt{r}}(2^m-1)\right].$$

Proof. The number of codewords of weight $n\omega$ is given by $N(G,n\omega) = \sum_{w\in\mathcal{W}} \mathbb{1}_w(G)$, $\mathcal{W}$ being the set of all the words of weight $n\omega$ over GF_2^m and $\mathbb{1}_w(G)$ is the indicator function. Then the expectation is

$$\mathbb{E}\left(N(G,n\omega)\right) = \sum_{w\in\mathcal{W}} \mathbb{E}\left(\mathbb{1}_w(G)\right). \quad (2)$$

Because of the symmetry in the permutation of edges and due to uniform probability of all the possible edge labels on every edge, $\mathbb{1}_w(G)$ is independent of the word w and depends only on its weight. We fix w to a word with support set $\{1,\ldots,n\omega\}$ and its non-zero symbols are unity. Then Eqn(2) reduces to $\mathbb{E}\left(N(G,n\omega)\right) = \binom{n}{n\omega}(2^m-1)^{n\omega}\,\mathbb{E}\left(\mathbb{1}_w(G)\right)$. Now,

$$\mathbb{E}\left(\mathbb{1}_w(G)\right) = \frac{\text{number of graphs for which } w \text{ is a codeword}}{\text{total number of graphs}}.$$

The total number of graphs is given by $(n\mathtt{l})!|\,\mathrm{GL}_2^m\,|^{n\mathtt{l}}$. The number of graphs for which w is a codeword is given by

$$(n\mathtt{l} - n\mathtt{l}\omega)!(n\mathtt{l}\omega)!|\,\mathrm{GL}_2^m\,|^{n\mathtt{l}-n\mathtt{l}\omega}\mathrm{coef}\left(p_m(y)^{\frac{n\mathtt{l}}{\mathtt{r}}}, y^{n\mathtt{l}\omega}\right).$$

The factorial terms correspond to permuting the edges carrying zero value and non-zero value. The term $|\,\mathrm{GL}_2^m\,|^{n\mathtt{l}-n\mathtt{l}\omega}$ takes care of the fact that we can put any edge label on the edges carrying the value zero. To describe the polynomial $p_m(y)$, we make the following quantity $F_{\mathtt{r}}$ for $\mathrm{EGL}\,(n,\mathtt{l},\mathtt{r},m)$ and $\mathrm{EGF}\,(n,\mathtt{l},\mathtt{r},m)$ respectively:

$$\begin{aligned} F_{\mathtt{r}} &= \left|\left\{(M_1\ldots,M_{\mathtt{r}}) : \sum_{i=1}^{\mathtt{r}} M_i x_i = 0, M_i \in \mathrm{GL}_2^m, x_i \in \mathrm{GF}_2^m\right\}\right|, \\ &= \frac{|\,\mathrm{GL}_2^m\,|^{\mathtt{r}}}{2^m}\left(1 + \frac{(-1)^{\mathtt{r}}}{(2^m-1)^{\mathtt{r}-1}}\right). \end{aligned}$$

$$\begin{aligned} F_{\mathtt{r}} &= \left|\left\{(M_1\ldots,M_{\mathtt{r}}) : \sum_{i=1}^{\mathtt{r}} M_i x_i = 0, M_i \in \mathrm{GF}^*(2^m), x_i \in \mathrm{GF}^*(2^m)\right\}\right|, \\ &= \frac{2^m-1}{2^m}\left((-1)^{\mathtt{r}} + (2^m-1)^{\mathtt{r}-1}\right). \end{aligned}$$

Then the polynomial $p_m(y)$ is given by $p_m(y) = 1 + \sum_{i=1}^{\mathtt{r}}\binom{\mathtt{r}}{i}F_i y^i, = \frac{1}{2^m}\left[(1+|\,\mathrm{GL}_2^m\,|y)^{\mathtt{r}} + \left(1 - \frac{|\,\mathrm{GL}_2^m\,|y}{2^m-1}\right)^{\mathtt{r}}(2^m-1)\right]$. In summary,

$$\mathbb{E}\left(\mathbb{1}_w(G)\right) = \frac{\mathrm{coef}\left(p_m(y)^{\frac{n\mathtt{l}}{\mathtt{r}}}, y^{n\mathtt{l}\omega}\right)}{\binom{n\mathtt{l}}{n\mathtt{l}\omega}|\,\mathrm{GL}_2^m\,|^{n\mathtt{l}\omega}}. \quad (3)$$

Substituting Eqn(3) in the expression for $\mathbb{E}\left(N(G,n\omega)\right)$ in Eqn(**??**) gives the desired result. □

Using similar arguments we obtain the average weight distribution for the ensemble $\mathrm{EGF}\,(n,\mathtt{l},\mathtt{r},m)$:

Lemma 3.2 (Average Weight Distribution of EGF$\,(n,\mathtt{l},\mathtt{r},m)$): For $\mathrm{EGF}(n,\mathtt{l},\mathtt{r},m)$, the average weight distribution is

$$\mathbb{E}[N(G,n\omega)] = \frac{\binom{n}{n\omega}}{\binom{n\mathtt{l}}{n\mathtt{l}\omega}(2^m-1)^{n(\mathtt{l}-1)\omega}} \mathrm{coef}\left(p_m(y)^{\frac{n\mathtt{l}}{\mathtt{r}}}, y^{n\mathtt{l}\omega}\right), \quad (4)$$

$$\text{with} \quad p_m(y) = \frac{1}{2^m}\left[(1+(2^m-1)y)^{\mathtt{r}} + (1-y)^{\mathtt{r}}(2^m-1)\right]. \quad (5)$$

IV. Expectation of the Binary Weight Distribution

In this section we derive average binary weight distributions.

Lemma 4.1 (Binary Weight Distribution of EGL$\,(n,\mathtt{l},\mathtt{r},m)$): Consider the ensemble $\mathrm{EGL}\,(n,\mathtt{l},\mathtt{r},m)$. Let $N_b\,(G,nm\omega)$ denote the binary weight distribution of a randomly chosen code G. Then the average $\mathbb{E}\left(N_b\,(G,nm\omega)\right)$ is given by

$$\sum_{i=n\omega}^{\min(n,nm\omega)} \frac{\binom{n}{i}\mathrm{coef}\left(((1+x)^m-1)^i, x^{nm\omega}\right)\mathrm{coef}\left(p_m(y)^{\frac{n\mathtt{l}}{\mathtt{r}}}, y^{\mathtt{l}i}\right)}{\binom{n\mathtt{l}}{i\mathtt{l}}|\,\mathrm{GL}_2^m\,|^{\mathtt{l}i}}, \quad (6)$$

where $\omega \in (0,1)$.

Proof. The average binary weight distribution is given by

$$\mathbb{E}\left(N_b\,(G,nm\omega)\right) = \sum_{i=n\omega}^{\min(n,nm\omega)} g(i,nm\omega)\cdot \mathrm{P}\left(\text{given weight-}i\text{ word is cwd of G}\right), \quad (7)$$

where $g(i,nm\omega)$ denotes the number of words with weight i whose binary weight is $nm\omega$ and is given by

$$g(i,nm\omega) = \binom{n}{i}\mathrm{coef}\left(((1+x)^m-1)^i, x^{nm\omega}\right). \quad (8)$$

Combining Eqn(3) and Eqn(8) gives Eqn(6). □

Using similar arguments, we obtain the average binary weight distribution of the ensemble $\mathrm{EGF}(n,\mathtt{l},\mathtt{r},m)$:

Lemma 4.2 (Binary Weight Distribution of EGF $(n,\mathtt{l},\mathtt{r},m)$): Let $N_b(G,nm\omega)$ denote the binary weight distribution of a code G randomly chosen from $\mathrm{EGF}(n,\mathtt{l},\mathtt{r},m)$. Then $\mathbb{E}(N_b(G,nm\omega))$ is given by

$$\sum_{i=n\omega}^{\min(n,nm\omega)} \frac{\binom{n}{i}\mathrm{coef}\left(((1+x)^m-1)^i,x^{nm\omega}\right)\mathrm{coef}\left(p_m(y)^{\frac{n\mathtt{l}}{\mathtt{r}}},y^{\mathtt{l}i}\right)}{\binom{n\mathtt{l}}{i\mathtt{l}}(2^m-1)^{\mathtt{l}i}},$$

where $\omega\in(0,1)$ and $p_m(y)$ is defined by Eqn(5).

Let us recall the Hayman method [18], [19] for approximating the term $\mathrm{coef}(q(y)^n,y^{n\omega})$ for large n, where $q(y)$ is a finite degree polynomial satisfying appropriate technical conditions.

Lemma 4.3 (Hayman Method): Let $q(y)=\sum_i q_i y^i$ be a polynomial with non negative coefficients such that $q_0\neq 0$ and $q_1\neq 0$. Define $a_q(y):=y\frac{dq(y)}{dy}\frac{1}{q(y)}$ and $b_q(y):=y\frac{da_q(y)}{dy}$. Then for $n\to\infty$ so that $n\omega\in\mathbb{N}$

$$\mathrm{coef}(q(y)^n,y^{n\omega})=\frac{q(y_\omega)^n}{y_\omega^{n\omega}\sqrt{2\pi n b_q(y_\omega)}}(1+o(1)),\qquad (9)$$

where the term $o(1)$ converges to zero and y_ω is the unique positive solution of $a_q(y)=\omega$.

Note that $p_m(y)$ satisfies technical conditions of Lemma 4.3 for $m\geq 2$. Therefore, we have the following estimation:

Lemma 4.4 (Average Weight Distribution for $m\geq 2$): Consider the regular ensemble $\mathrm{EGL}(n,\mathtt{l},\mathtt{r},m)$, where $m\geq 2$. The average weight distribution is given by

$$\mathbb{E}(N(G,n\omega))=\frac{\sqrt{\mathtt{r}}}{\sqrt{2\pi n b_{p_m}(x_\omega)}}\cdot$$
$$e^{n\left(\omega\ln(2^m-1)-h(\omega)(\mathtt{l}-1)+\frac{\mathtt{l}}{\mathtt{r}}\ln(p_m(y_\omega))-\mathtt{l}\omega\ln\left(|\mathrm{GL}_2^m|\right)-\mathtt{l}\omega\ln(x_\omega)\right)},\qquad (10)$$

where x_ω is the solution of $a_{p_m}(x)=\mathtt{r}\omega$ and $h(\omega)=-(\omega\ln\omega+(1-\omega)\ln(1-\omega))$ and $\ln\omega$ is the natural logarithm of ω.

Proof. The proof is straightforward and uses the Stirling approximation of $\binom{n}{n\omega}$, Lemma 3.1 and Lemma 4.3. □

A similar result also holds for $\mathrm{EGF}(n,\mathtt{l},\mathtt{r},m)$.

V. Growth Rate

Let us characterize the growth rate of the binary weight distribution of $\mathrm{EGL}(n,\mathtt{l},\mathtt{r},m)$ and $\mathrm{EGF}(n,\mathtt{l},\mathtt{r},m)$ as $m\to\infty$. We derive it by observing that, for both ensembles, the average binary weight distribution $\mathbb{E}(N_b(G,nm\omega))$ can be written as

$$\sum_{i=n\omega}^{\min(n,nm\omega)} \frac{\binom{n}{i}\mathrm{coef}\left(((1+x)^m-1)^i,x^{nm\omega}\right)\mathrm{coef}\left(p_m(y)^{\frac{n\mathtt{l}}{\mathtt{r}}},y^{\mathtt{l}i}\right)}{\binom{n\mathtt{l}}{i\mathtt{l}}A^{\mathtt{l}i}},\qquad (11)$$

where

$$p_m(y)=\frac{1}{2^m}\left[(1+Ay)^{\mathtt{r}}+\left(1-\frac{Ay}{2^m-1}\right)^{\mathtt{r}}(2^m-1)\right].$$

Here $A=|\mathrm{GL}_2^m|$ for $\mathrm{EGL}(n,\mathtt{l},\mathtt{r},m)$ and $A=2^m-1$ for $\mathrm{EGF}(n,\mathtt{l},\mathtt{r},m)$.

Let us denote the summation term of Eqn(11) corresponding to index i by S_i. We normalize i by n and write $i=\gamma n$. Let $\beta_m(\omega)$ be the growth rate of the average binary weight distribution. To derive the expression of $\beta_m(\omega)$, note that $\min(1,m\omega)=1$ for a fixed non-zero ω when n gets large. Thus, for m large enough, we obtain that

$$\beta_m(\omega)=\frac{1}{m}\max\left(\lim_{n\to\infty}\frac{\log(S_{n\omega})}{n},\sup_{\gamma\in(\omega,1)}\alpha_m(\omega,\gamma),\lim_{n\to\infty}\frac{\log(S_n)}{n}\right),\qquad (12)$$

where

$$\alpha_m(\omega,\gamma)=\inf_{x>0}\inf_{y>0}\{-(\mathtt{l}-1)h(\gamma)-\gamma\mathtt{l}\log(A)-(m\omega-\gamma)\log(x)$$
$$+\gamma\log\left(\frac{(1+x)^m-1}{x}\right)+\frac{\mathtt{l}}{\mathtt{r}}\log(p_m(y))-\mathtt{l}\gamma\log(y)\Bigg\}\qquad (13)$$

Here we used the fact that $\mathrm{coef}\left(((1+x)^m-1)^i,x^{nm\omega}\right)=\mathrm{coef}\left(\left(\frac{(1+x)^m-1}{x}\right)^i,x^{nm\omega-i}\right)$. For $\gamma\in(\omega,1)$, the values of x and y corresponding to the infimum in Eqn(13) satisfy two following conditions:

$$\frac{x(1+x)^{m-1}}{(1+x)^m-1}=\frac{\omega}{\gamma}\qquad (14)$$

$$Ay\frac{(1+Ay)^{\mathtt{r}-1}-\left(1-\frac{Ay}{2^m-1}\right)^{\mathtt{r}-1}}{(1+Ay)^{\mathtt{r}}+\left(1-\frac{Ay}{2^m-1}\right)^{\mathtt{r}}(2^m-1)}=\gamma,\qquad (15)$$

Let us compute the solutions of Eqns(14, 15), when $m\to\infty$.

Lemma 5.1: Let x_m and y_m be the solutions of Eqn(14) and Eqn(15). For increasing values of m, the solution to Eqn(14) and Eqn(15) is given by

$$x_m=x^*\left(1+O\left(\left(\frac{\gamma}{\gamma-\omega}\right)^{-m}\right)\right),\quad x^*=\frac{\omega}{\gamma-\omega},\qquad (16)$$

$$y_m=y^*(1+o(1)),\quad y^*=\frac{1}{A}\left(\frac{\gamma 2^m}{1-\gamma}\right)^{\frac{1}{\mathtt{r}}}.\qquad (17)$$

Proof. Let x_m be the solution of Eqn(14). Note that for large values of m, $(1+x)^m-1\approx(1+x)^m$. Using this we get the desired expression for x_m. Now, let y_m be the solution of Eqn(15). Let us make the following assumption on the solution y_m:

$$Ay_m=o(2^m-1),\qquad Ay_m=\Omega(m).\qquad (18)$$

Then the numerator and the denominator of Eqn(15) become

$$Ay_m(1+Ay_m)^{\mathtt{r}-1}-Ay_m\left(1-\frac{Ay_m}{2^m-1}\right)^{\mathtt{r}-1}=(Ay_m)^{\mathtt{r}}+O(Ay_m)^{\mathtt{r}-1};$$

$$(1+Ay_m)^{\mathtt{r}}+\left(1-\frac{Ay_m}{2^m-1}\right)^{\mathtt{r}}(2^m-1)=(Ay_m)^{\mathtt{r}}+2^m+O((Ay_m)^{\mathtt{r}-1}).$$

Therefore, Eqn(15) becomes $\frac{(Ay_m)^{\mathtt{r}}}{(Ay_m)^{\mathtt{r}}+2^m}=\gamma+O\left(\frac{1}{Ay_m}\right)$. Thus the solution is $y_m=\frac{1}{A}\left(\frac{\gamma 2^m}{1-\gamma}\right)^{\frac{1}{\mathtt{r}}}(1+o(1))$. Note that it satisfies the conditions given by Eqn(18). □

Now we have the following result:

Lemma 5.2: Let $\gamma\in(\omega,1)$. Then there is only one positive root of Eqn(14) and Eqn(15).

Proof. Rewrite Eqn(14) as $\sum_{j=0}^{m-1}\binom{m-1}{j}x^{j+1} - \frac{\omega}{\gamma}\sum_{j=1}^{m}\binom{m}{j}x^j = 0$. By changing the index of the first summation term, we get $\sum_{j=1}^{m}\left(1-\frac{\omega}{\gamma}\frac{m}{j}\right)\binom{m-1}{j-1}x^j = 0$. For $j > \frac{m\omega}{\gamma}$, the coefficients are positive, otherwise negative as $\gamma > \omega$. So, there is only one sign change and by Descarte's rule of sign, there is only one positive root to Eqn(14). Now, rewrite Eqn(15) as

$$-\gamma 2^m + \sum_{j=1}^{\mathtt{r}}\binom{\mathtt{r}-1}{j-1}y^jA^j\left(1+\frac{(-1)^j}{(2^m-1)^{j-1}}\right)\left(1-\frac{\gamma\mathtt{r}}{j}\right) = 0.$$

For $j > \gamma\mathtt{r}$ the coefficients become positive as $\gamma < 1$. Again, there is only one sign change and by Descarte's rule of sign there is only one positive solution to the equation. □

We now derive a lemma concerning the evaluation of polynomials which will be very useful later:

Lemma 5.3: Let x_m and y_m be the solutions of Eqn(14) and Eqn(15) given in Lemma 5.1. Then for $\gamma \in [\omega, 1)$

$$\begin{aligned} p_m(y_m) &= p_m(y^*)(1+o(1)), \\ (1+x_m)^m - 1 &= ((1+x^*)^m - 1)\,e^{o(m)}. \end{aligned}$$

Proof. As the constant term in $p_m(y)$ is 1, we obtain

$$p_m(y_m) = p_m(y)\left(1+\frac{p_m(y^*)-1}{p_m(y^*)}o(1)\right) = p_m(y^*)(1+o(1)),$$

Rewrite the polynomial corresponding to x_m as

$$(1 + x_m)^m - 1 = \sum_{i=1}^{m}\binom{m}{i}(x^*)^i(1 + o(1))^i.$$

The term $(1+o(1))^i$ is largest for $i = m$ and it is equal to $(1+o(1))^m = e^{mo(1)} = e^{o(m)}$. This proves the lemma. □

We start the final calculation and derive the expression for $\sup_{\gamma\in(\omega,1)}\alpha_m(\omega,\gamma)$ for large m by deriving lower and upper bounds and by showing that they are tight as $m \to \infty$.

A. Upper Bound on the Supremum of $\alpha_m(\gamma,\omega)$

To derive the upper bound to $\alpha_m(\omega,\gamma)$, for a fixed γ we can substitute any positive value of x and y on the RHS of Eqn(13). We choose $x = x^* = \frac{\omega}{\gamma-\omega}$, $y = y^* = \frac{1}{A}\left(\frac{\gamma 2^m}{1-\gamma}\right)^{\frac{1}{\mathtt{r}}}$. Now, for $x^* > 0$,

$$\begin{aligned} \gamma\log\left(\frac{(1+x^*)^m-1}{x^*}\right) &\le m\gamma\log(1+x^*) - \gamma\log(x^*) \\ &= m\gamma\log\left(\frac{\gamma}{\gamma-\omega}\right) - \gamma\log\left(\frac{\omega}{\gamma-\omega}\right). \quad (19) \end{aligned}$$

We obtain the following upper bound on $p_m(y^*)$:

$$p_m(y^*) = \frac{\gamma}{1-\gamma}\left[\left(1+\left(\frac{1-\gamma}{\gamma 2^m}\right)^{\frac{1}{\mathtt{r}}}\right)^{\mathtt{r}} + \left(\left(\frac{1-\gamma}{\gamma 2^m}\right)^{\frac{1}{\mathtt{r}}} - \frac{1}{2^m-1}\right)^{\mathtt{r}}(2^m-1)\right]. \quad (20)$$

Assume m large, then $\gamma \in (\omega, \min(1, m\omega)) = (\omega, 1)$ and

$$p_m(y^*) \le \frac{\gamma}{1-\gamma}\left[\left(1+\left(\frac{1-\omega}{2\omega}\right)^{\frac{1}{\mathtt{r}}}\right)^{\mathtt{r}} + \left(\frac{1-\omega}{\omega}\right)^{\mathtt{r}}\right]. \quad (21)$$

Substituting Eqns(19, 21) in Eqn(13), we obtain

$$\begin{aligned} \alpha_m(\gamma,\omega) \le \gamma\log\left(\frac{\gamma}{\gamma-\omega}\right) - \omega\log\left(\frac{\omega}{\gamma-\omega}\right) - \frac{\gamma\mathtt{l}}{\mathtt{r}} \\ + \frac{1}{m}\left[-(\mathtt{l}-1)h(\gamma) + \frac{\mathtt{l}}{\mathtt{r}}(1-\gamma)\log\left(\frac{\gamma}{1-\gamma}\right) + \right. \\ \left. \frac{\mathtt{l}}{\mathtt{r}}\log\left(\left(1+\left(\frac{1-\omega}{2\omega}\right)^{\frac{1}{\mathtt{r}}}\right)^{\mathtt{r}} + \left(\frac{1-\omega}{\omega}\right)^{\mathtt{r}}\right)\right] \end{aligned}$$

Note that the term normalized by m can be upper bounded by a constant dependent only on ω. This is because for $\gamma \in (\omega, 1)$, $(1-\gamma)\log(\gamma) \le 0$ and $-(1-\gamma)\log(1-\gamma) \le 1$. Hence,

$$\alpha(\omega,\gamma) \triangleq \lim_{m\to\infty}\alpha_m(\omega,\gamma) \le \bar{\alpha}(\omega,\gamma),$$

where

$$\bar{\alpha}(\omega,\gamma) \triangleq \gamma\log\left(\frac{\gamma}{\gamma-\omega}\right) - \omega\log\left(\frac{\omega}{\gamma-\omega}\right) - \frac{\mathtt{l}}{\mathtt{r}}\gamma\log(2). \quad (22)$$

The derivative of $\bar{\alpha}(\omega,\gamma)$ over γ is $\frac{\partial\bar{\alpha}(\omega,\gamma)}{\partial\gamma} = \log\left(\frac{\gamma}{\gamma-\omega}\right) - \frac{\mathtt{l}}{\mathtt{r}}\log(2)$. and becomes zero for $\gamma^* = \frac{\omega}{1-2^{-\mathtt{l}/\mathtt{r}}}$. The second derivative is $\frac{\partial^2\bar{\alpha}(\omega,\gamma)}{\partial\gamma^2} = \frac{-\omega}{\gamma(\gamma-\omega)}$. So, γ^* is indeed a maximum provided $\gamma^* < 1$. This means that for $\omega \le 1-2^{-\mathtt{l}/\mathtt{r}}$, γ^* is maximum. Otherwise, the maximum is achieved at $\gamma = 1$. We obtain the following bound

$$\sup_{\gamma\in(\omega,1)}\alpha(\omega,\gamma) \le \begin{cases} -\omega\log(2^{\mathtt{l}/\mathtt{r}}-1), & 0 \le \omega < 1-2^{-\mathtt{l}/\mathtt{r}}, \\ h(\omega) - \frac{\mathtt{l}}{\mathtt{r}}\log_e(2), & 1-2^{-\mathtt{l}/\mathtt{r}} \le \omega \le 1. \end{cases} \quad (23)$$

In order to obtain the upper bound on $\beta_m(\omega)$, we compute the end terms $i = \omega n$ and $i = n$ of summation in Eqn(11). Let us first consider $i = \omega n$ and observe that $\mathrm{coef}\left(((1+x)^m-1)^{n\omega}, x^{nm\omega}\right) = 1$. This gives

$$\begin{aligned} \lim_{n\to\infty}\frac{\log(S_{n\omega})}{nm} = \frac{1}{m}\left(-(\mathtt{l}-1)h(\omega) - \mathtt{l}\omega\log(A)\right) \\ + \inf_{y>0}\frac{1}{m}\left\{\frac{\mathtt{l}}{\mathtt{r}}\log(p_m(y)) - \mathtt{l}\omega\log(y)\right\}. \quad (24) \end{aligned}$$

From Lemma 5.1, we know that y_m defined in Eqn(17) corresponds to the infimum. From Eqn(20),

$$p_m(y^*) = \frac{\omega}{1-\omega}\left[\left(1+\left(\frac{1-\omega}{\omega 2^m}\right)^{\frac{1}{\mathtt{r}}}\right)^{\mathtt{r}} + \left(\left(\frac{1-\omega}{\omega 2^m}\right)^{\frac{1}{\mathtt{r}}} - \frac{1}{2^m-1}\right)^{\mathtt{r}}(2^m-1)\right].$$

We obtain $p_m(y^*) = \frac{\omega}{1-\omega}(1+o(1))$. Combining these calculations, substituting them in Eqn(24), and letting $m \to \infty$,

$$\lim_{m\to\infty}\lim_{n\to\infty}\frac{\log(S_{n\omega})}{nm} = -\frac{\mathtt{l}\omega}{\mathtt{r}}. \quad (25)$$

Now, as the coef term corresponding to $p_m(y)$ is given by

$$\mathrm{coef}\left(p_m(y)^{\frac{\mathtt{l}n}{\mathtt{r}}}, y^{n\mathtt{l}}\right) = \left(\frac{A^{\mathtt{r}}}{2^m}\left(1+\frac{(-1)^{\mathtt{r}}}{(2^m-1)^{\mathtt{r}-1}}\right)\right)^{\frac{\mathtt{l}n}{\mathtt{r}}},$$

the growth rate $\lim_{n\to\infty}\frac{\log(S_n)}{nm}$ is

$$\frac{\log\left((1+x_m)^m-1\right)}{m} - \omega\log(x_m) - \frac{\mathtt{1}}{\mathtt{r}} + \frac{\mathtt{1}}{m\mathtt{r}}\log\left(1+\frac{(-1)^{\mathtt{r}}}{(2^m-1)^{\mathtt{r}-1}}\right),$$

$x_m = x^*(1+o(1))$ being given by Eqn(16). From Lemma 5.3, $(1+x_m)^m-1 = \left((1+x^*)^m-1\right)e^{o(m)}$. This gives us

$$\lim_{n\to\infty}\frac{\log(S_n)}{nm} = h(\omega)-\frac{\mathtt{1}}{\mathtt{r}}. \qquad (26)$$

Finally, we state the upper bound on $\beta_m(\omega)$ when $m\to\infty$.

Lemma 5.4:

$$\beta(\omega) \leq \begin{cases} -\omega\log(2^{\mathtt{1}/\mathtt{r}}-1), & 0\leq\omega<1-2^{-\mathtt{1}/\mathtt{r}}, \\ h(\omega)-\frac{\mathtt{1}}{\mathtt{r}}, & 1-2^{-\mathtt{1}/\mathtt{r}}\leq\omega\leq 1. \end{cases}$$

Proof. By Eqns(22), (25) and (26), we observe that for $\omega\leq 1-2^{-\mathtt{1}/\mathtt{r}}$, the bound in Eqn(22) gives the maximum as it is positive and other two are negative. For $\omega>1-2^{-\mathtt{1}/\mathtt{r}}$, the bound in Eqn(22) and the growth rate of S_n in Eqn(26) coincide. Consider the difference between the bound in Eqn(22) and Eqn(25) and denote it by $\delta(\omega)$. Then $\delta(\omega)=h(\omega)-(1-\omega)\frac{\mathtt{1}}{\mathtt{r}}$. Its derivative $\frac{d\delta(\omega)}{d\omega} = \frac{1}{\log_e(2)}\left(\log_e\left(\frac{1-\omega}{\omega}\right)-\frac{\mathtt{1}}{\mathtt{r}}\log_e(2)\right)$, which is zero for

$$\omega = \frac{1}{1+2^{\mathtt{1}/\mathtt{r}}}.$$

The second derivative is equal to $\frac{d^2\delta(\omega)}{d\omega^2} = \frac{-1}{\log_e(2)\omega(1-\omega)}$. Thus, the first derivative is a strictly decreasing function of ω and it is negative for $\omega > 1/\left(1+2^{\mathtt{1}/\mathtt{r}}\right)$. As $\delta(1)=0$, $\delta(\omega)\geq 0$ for $\omega > 1/\left(1+2^{\mathtt{1}/\mathtt{r}}\right)$. Now,

$$\frac{1}{1+2^{\mathtt{1}/\mathtt{r}}} < 1-2^{-\mathtt{1}/\mathtt{r}},$$

we obtain that for $\omega > 1-2^{-\mathtt{1}/\mathtt{r}}$, the bound in Eqn(22) is greater than growth rate of S_n given in Eqn(26). □

B. Lower Bound on the Supremum of $\alpha_m(\omega)$

By using the upper bound, we choose carefully the values of γ for a fixed ω in Eqn(13), obtain a lower bound on the growth rate and show that it matches with the upper bound. For $\omega\geq 1-2^{-\mathtt{1}/\mathtt{r}}$, we choose $\gamma=1$. So, the lower bound is given by Eqn(26) which matches with the upper bound. For $\omega<1-2^{-\mathtt{1}/\mathtt{r}}$, we choose $\gamma=\frac{\omega}{1-2^{-\frac{\mathtt{1}}{\mathtt{r}}}}$. By using Lemmas 5.1, 5.3 and Eqn(20) in the evaluation of RHS of Eqn(13), we obtain the expression which is equal to $\bar{\alpha}\left(\omega,\frac{\omega}{1-2^{-\mathtt{1}/\mathtt{r}}}\right)$, where $\bar{\alpha}(\omega,\gamma)$ is defined in Eqn(22). This matches with the upper bound. Thus, the upper bound on $\beta(\omega)$ is tight. This proves Theorem 1.1.

VI. Discussion of the Obtained Result

In this paper, we have shown that when $n\longrightarrow\infty$ and $m\longrightarrow\infty$, the growth rates of regular LDPC ensembles over finite fields and over the general linear group have the following form: it is the straight line for normalized binary weights smaller than a critical value $1-2^{-\mathtt{1}/\mathtt{r}}$ and is equal to the growth rate of the binomial distribution for weights greater or equal than $1-2^{-\mathtt{1}/\mathtt{r}}$. However, does such a pessimistic result on the growth rate indicate that the channel capacity under ML decoding cannot be achieved with non-regular LDPC codes? Our further analysis shows that a regular LDPC ensemble over finite fields or over the generalized linear group contains an exponentially small number of codes having an exponentially large number of codewords of linear weight, which, contributing into the average weight distribution of the ensemble, produce such a straight-line behavior. The details of the computation are beyond the scope of this paper and will be given in its extended version [1]. Nevertheless, this justification shows that it still might be possible to show the capacity-approaching property of LDPC codes over large alphabets under ML decoding, either by doing an appropriate expurgation or by applying another averaging method.

References

[1] I. Andriyanova, V. Rathi, and J. Tillich, "Weight distributions of non-binary LDPC codes," to be submitted.

[2] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, Massachusetts: M.I.T. Press, 1963.

[3] C. Berrou and M. Jézéquel, "Non binary convolutional codes for turbo-coding," *Electronic Letters*, vol. 35, no. 1, pp. 39–40, January 1999.

[4] C. Berrou, M. Jézéquel, C. Douillard, and S. Kerouédan, "The advantages of non-binary turbo-codes," in *Information Theory Workshop ITW'01*, Cairns, Australia, September 2001, pp. 61–63.

[5] J. Boutros, G. Caire, E. Viterbo, H. Sawaya, and S. Vialle, "Turbo code at 0.03 dB from capacity limit," in *IEEE International Symposium on Information Theory*, Lausanne, Switzerland, June 30–July 5 2002, conference, p. 56.

[6] H. Sawaya and J. Boutros, "Irregular turbo-codes with symbol-based iterative decoding," in *3rd International Symposium on Turbo-codes*, Brest, France, September 2003, pp. 407–410.

[7] M. Davey and D. MacKay, "Low density parity check codes over gf(q)," *IEEE Communications Letters*, vol. 2, pp. 165–167, June 1998.

[8] X. Hu, "Low-delay low-complexity error-correcting codes on sparse graphs," Ph.D. dissertation, EPFL, Lausanne, Switzerland, 2002.

[9] E. E. X. Hu, "Binary representation of cycle tanner-graph gf(2^b) codes," in *ICC'04*, Paris, France, June 2004.

[10] X. Hu, E. Eleftheriou, and D. Arnold, "Regular and irregular progressive edge-growth Tanner graphs," *IEEE Trans. on Inform. Theory*, vol. 51, no. 1, pp. 386–398, January 2005.

[11] V. Rathi and R. Urbanke, "Density evolution, thresholds and the stability condition for non-binary ldpc codes," *IEEE Trans. on Comm.*, December 2005.

[12] I. Andriyanova and J. Tillich, "A family of non-binary TLDPC codes: density evolution, convergence and thresholds," in *ISIT'07*, Nice, France, June 2007, pp. 1216–1220.

[13] A. Bennatan, "The application of LDPC codes to new problems in communications," Ph.D. dissertation, Tel Aviv University, 2006.

[14] F. F. G. Como, "Average spectra and minimum distances of low density parity check codes over cyclic groups," 2007, submitted.

[15] E. Hof, I. Sason, and S. Shamai, "Gallager-type bounds for non-binary linear block codes over memoryless symmetric channels," 2008, submitted ot the IEEE transactions on information theory.

[16] K. Kasai, C. Poulliat, D. Declercq, T. Shibuya, and K. Sakaniwa, "Weight distribution of non-binary ldpc codes," in *Proceedings of ISITA*, December 2008.

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

[18] P. Flajolet and R. Sedgewick, "The average case analysis of algorithms: Saddle point asymptotics," RR 2376, Tech. Rep., oct 1994.

[19] D. Gardy, "Some results on the asymptotic behavior of coefficients of large powers of functions," *Discrete Mathematics*, vol. 139, pp. 189–217, 1995.