Weight Distributions of Non-binary LDPC Codes

Kenta Kasai, Charly Poulliat, David Declercq, Kohichi Sakaniwa

IEICE TRANS. FUNDAMENTALS, VOL.E94–A, NO.4 APRIL 2011

PAPER

Weight Distributions of Non-binary LDPC Codes

Kenta KASAI[†a)], ***Member***, **Charly POULLIAT**[††b)], **David DECLERCQ**[††c)], ***Nonmembers***, ***and*** **Kohichi SAKANIWA**[†d)], ***Fellow***

SUMMARY In this paper, we study the average symbol and bit-weight distributions for ensembles of non-binary low-density parity-check codes defined on GF(2^p). Moreover, we derive the asymptotic exponential growth rate of the weight distributions in the limit of large codelength. Interestingly, we show that the normalized typical minimum distance does not monotonically increase with the size of the field.

key words: *non-binary low-density parity-check code, weight distribution, Galois fields*

1. Introduction

In 1963, Gallager invented low-density parity-check (LDPC) codes [1]. Due to the sparseness of the code representation, LDPC codes are efficiently decoded by sum-product decoders [2] or belief propagation (BP) decoders [3]. Using a powerful analytical method called *density evolution* [3] that was proposed by Richardson and Urbanke, messages of BP decoding are statistically evaluated and codes can be optimized for best decoding thresholds. The optimized LDPC codes [4] exhibit the decoding performance at a rate very close to the Shannon capacity.

Non-binary LDPC codes were invented by Gallager [1]. Davey and MacKay [5] found that non-binary LDPC codes can outperform binary LDPC codes. Non-binary LDPC codes have captured much attention recently due to their decoding performance [6]–[10]. The $(2, d_c)$-regular non-binary LDPC codes defined on GF(2^p) are empirically known as the best codes for $2^p \geq 64$, especially for short codelength. Poulliat et al. optimized $(2, d_c)$-regular non-binary LDPC codes by considering binary images of GF(2^p) symbols. However, the main shortcoming of non-binary LDPC codes is their decoding complexity and requirements of large memories. Reduced complexity algorithms for decoding non-binary LDPC codes have recently been proposed [11]. Recently, the decoder for non-binary LDPC codes was implemented on general-purpose computing on graphics processing units (GPGPUs) [12], which runs much faster than those implemented on CPUs.

The weight distributions of linear codes play very important roles in analysis of the decoding performance. Specifically, for LDPC codes, the bound of the thresholds for the ML decoding [1], [13], and the error floors [14], [15] for BP decoding were studied using the weight distributions.

Studies on weight distributions for binary LDPC codes date back to Gallager's landmark PhD thesis [1]. Gallager derived the average weight distributions of LDPC code ensembles and empirically showed that the typical minimum distance [1], for fixed rates, grows with the weight of rows and and columns of the parity-check matrices. In [16], the weight distributions of various classes of regular LDPC code ensembles were derived. In [17], the weight distributions of irregular LDPC code ensembles were derived. In [14] and [15], the exponential growth rate of the weight distribution of the standard irregular code ensembles [18] were derived. Recently, in [19], the authors investigated the weight distributions of multi-edge type LDPC code ensembles.

Studies on weight distributions for non-binary LDPC codes also date back to [1]. Gallager derived symbol-weight distribution of Gallager code ensembles defined on $\mathbb{Z}/q\mathbb{Z}$ and showed that the minimum distance grows linearly with codelength when the variable node degree is greater than 2. Hu [20] derived the asymptotic bit-weight distributions for random parity-check code ensembles.

For the transmission over the binary input channels, we restrict ourselves to considering non-binary LDPC codes over GF(q) with $q = 2^p$. Once the primitive element of GF(2^p) is fixed, each symbol in GF(2^p) can be represented as a binary sequence of length p. With this binary representation, the weight distributions of the non-binary LDPC codes can be considered not only in terms of the symbol-weight but also in terms of the bit-weight. In this paper, we derive the average weight distributions of the symbol and bit-weight for non-binary LDPC code ensembles defined on GF(2^p). We derive the asymptotic growth rate and the condition for the exponentially few average number of codewords of small linear weight.

The rest of this paper is organized as follows. In Sect. 2, we define non-binary LDPC codes and their ensembles. Section 3 derives the average symbol and bit-weight distributions. Section 4 investigates the asymptotic exponential growth rate of the average symbol and bit-weight distributions. Section 5 illustrates the numerical examples of the

Manuscript received April 30, 2010.
Manuscript revised November 14, 2010.

[†]The authors are with the Dept. of Communications and Integrated Systems, Tokyo Institute of Technology, Tokyo, 152-8552 Japan.
[††]The authors are with ETIS ENSEA/University of Cergy-Pontoise/CNRS, F-95000, Cergy-Pontoise, Cergy, France.
a) E-mail: kenta@comm.ss.titech.ac.jp
b) E-mail: poulliat@ensea.fr
c) E-mail: declercq@ensea.fr
d) E-mail: sakaniwa@comm.ss.titech.ac.jp
DOI: 10.1587/transfun.E94.A.1106

asymptotic growth rate of the average symbol and bit-weight distributions. Section 6 concludes this paper.

2. Non-binary LDPC Code Ensemble

Binary and non-binary LDPC codes are defined by bipartite graphs which are also referred to as Tanner graphs [18]. For a bipartite graph with N variable nodes and M check nodes, with some abuse of notation, we denote the v-th variable node and c-th check node by v and c, respectively.

The Tanner graph is said to have a degree distribution pair

$$\left(\lambda(x) = \sum_{i=2}^{d_v} \lambda_i x^{i-1}, \rho(x) = \sum_{j=2}^{d_c} \rho_j x^{j-1}\right)$$

if the fraction of edges incident to variable nodes of degree i is λ_i for $i = 2, \ldots, d_v$ and the fraction of edges incident to check nodes of degree j is ρ_j for $j = 2, \ldots, d_c$. Each edge $= (c, v)$ is labeled $h_{(c,v)} \in \mathrm{GF}(2^p)\backslash\{0\}$. For a given Tanner graph, we consider all $\mathrm{GF}(2^p)$-valued maps on each variable node v such that

$$x : v \mapsto x_v \in \mathrm{GF}(2^p).$$

A map x is said to be a codeword if the values of x satisfies all the check constraints. To be precise,

$$\sum_{v \in V_c} h_{(c,v)} x_v = 0 \text{ for } c = 1, \ldots, M,$$

where V_c is the set of variable nodes adjacent to the check node c. The symbol-weight $w(x)$ of x is defined by the number of non-zero values of x_v. To be precise

$$w(x) = |\{v \in \{1, \ldots, N\} \mid x_v \neq 0\}|.$$

The parameters $N, M, \rho(x)$ and $\lambda(x)$ are constrained to ensure that the number of edges on variable node and check node sides is consistent.

$$N \Big/ \int_0^1 \lambda(x)dx = M \Big/ \int_0^1 \rho(x)dx =: E, \tag{1}$$

where we denote the number of edges by E. The set of edges is denoted by $\mathtt{E}$.

Assume we are given the following parameters for the code construction. The codelength N, a degree distribution pair $(\lambda(x), \rho(x))$, and the Galois field $\mathrm{GF}(2^p)$ of size $q = 2^p$. With these parameters, we define the non-binary irregular LDPC code ensemble as an equiprobable set of the codes defined by the Tanner graphs which have N variable nodes, the degree distribution pair $(\lambda(x), \rho(x))$ and edges with labels uniformly and randomly chosen from $\mathrm{GF}(2^p)\backslash\{0\}$. The non-binary irregular LDPC code ensemble is denoted by $\mathcal{G}(N, \lambda(x), \rho(x), 2^p)$.

We consider the standard Tanner graph modeled with *sockets* [18]. Each variable (resp. check) node has i sockets, where i is the degree of the variable (resp. check) node. The sockets are aligned in arbitrary but fixed order. Variable and check nodes are connected via their sockets. Thus graph connection is specified by a permutation π on $[1, E]$ such that i-th variable socket connects to the $\pi(i)$-th check sockets. There are $E!$ possible ways of the edge connection consistent with $(\lambda(x), \rho(x))$. There are $(q-1)^E$ possible ways of choosing non-zero entries $\{h_{(c,v)}\}_{(c,v)\in\mathtt{E}}$.

Consequently, the number of codes in the ensemble $\mathcal{G}(N, \lambda(x), \rho(x), 2^p)$ is given by

$$|\mathcal{G}(N, \lambda(x), \rho(x), 2^p)| = E!(q-1)^E. \tag{2}$$

Furthermore, we define the design rate r as follows.

$$r := (N - M)/N = 1 - \frac{\int_0^1 \rho(x)dx}{\int_0^1 \lambda(x)dx}.$$

3. Weight Distribution of Non-binary LDPC Codes

In this section, we derive the average bit-weight and symbol-weight distribution of the non-binary irregular LDPC code ensemble $\mathcal{G}(N, \lambda(x), \rho(x), 2^p)$.

In order to transmit the codewords over the binary-input channels, we consider the binary-image of non-binary symbols. Once a primitive element α of $\mathrm{GF}(2^p)$ is fixed, each symbol is given a p-bit representation [21, pp.110]. For example, with a primitive element $\alpha \in \mathrm{GF}(2^3)$ such that $\alpha^3 + \alpha + 1 = 0$, each symbol is represented as $0 = (0, 0, 0)$, $1 = (1, 0, 0)$, $\alpha = (0, 1, 0)$, $\alpha^2 = (0, 0, 1)$, $\alpha^3 = (1, 1, 0)$, $\alpha^4 = (0, 1, 1)$, $\alpha^5 = (1, 1, 1)$ and $\alpha^6 = (1, 0, 1)$.

For a given Tanner graph G, we denote the number of codewords of symbol-weight and bit-weight ℓ in G by $A^G(\ell)$ and $A^G_{\mathrm{b}}(\ell)$, respectively. For the non-binary irregular LDPC code ensemble $\mathcal{G}(N, \lambda(x), \rho(x), 2^p)$, let $A(\ell)$ and $A_{\mathrm{b}}(\ell)$ be the average number of codewords of symbol-weight and bit-weight ℓ, respectively. Since each code in the ensemble $\mathcal{G} = \mathcal{G}(N, \lambda(x), \rho(x), 2^p)$ is given uniform probabilities, it follows that

$$A(\ell) = \sum_{G \in \mathcal{G}} A^G(\ell)/|\mathcal{G}|,$$
$$A_{\mathrm{b}}(\ell) = \sum_{G \in \mathcal{G}} A^G_{\mathrm{b}}(\ell)/|\mathcal{G}|.$$

3.1 Symbol-Weight Distribution for Non-binary LDPC Codes

We will derive the average symbol-weight distribution of the non-binary irregular LDPC code ensemble $\mathcal{G}(N, \lambda(x), \rho(x), 2^p)$. For readers who are unfamiliar with the enumeration technique developed for the weight distributions of LDPC code ensembles so far, we refer the readers to [1], [14], [16], [17].

Theorem 1: The average number of codewords $A(\ell)$ of symbol-weight ℓ for the non-binary irregular LDPC code ensemble $\mathcal{G} = \mathcal{G}(N, \lambda(x), \rho(x), 2^p)$ is given by

$$A(\ell) = \sum_{k\geq 0} \frac{\mathrm{coef}\left((Q(s,t)P(u))^N, t^\ell s^k u^k\right)}{\binom{E}{k}(q-1)^{E-k}},$$

$$Q(s,t) := \prod_{i=2}^{d_v}(1+ts^i)^{L_i}, \quad P(u) := \prod_{j=2}^{d_c} f_j(u)^{R_j},$$

$$f_j(u) := \frac{1}{q}\left((1+(q-1)u)^j + (q-1)(1-u)^j\right),$$

where $\mathrm{coef}(g(s,t,u), s^i t^j u^k)$ is the coefficient of a term $s^i t^j u^k$ in a polynomial $g(s,t,u)$. NL_i and NR_j are the number of variable and check nodes of degree i and j, respectively i.e.,

$$L_i = \frac{\lambda_i}{i\int_0^1 \lambda(x)dx}, R_j = \frac{\rho_j(1-r)}{j\int_0^1 \rho(x)dx} = \frac{\rho_j}{j\int_0^1 \lambda(x)dx}.$$

Note that $\sum_{j=2}^{d_c} R_j = 1-r$ and $\sum_{j=2}^{d_c} R_j N = M$.

Proof: We say an edge is active if the edge is incident to a variable node v such that $x_v \neq 0$. Each edge (c,v) can be viewed as a conveyer of the value $y_{(c,v)} := h_{(c,v)}x_v$ from the incident variable node v to the incident check node. The check node c determines whether it is satisfied or not only by the values $y_{(c,v)}$ which are conveyed along the connecting edges (c,v) for $v \in V_c$. To be precise, c is satisfied if

$$\sum_{v\in V_c} y_{(c,v)} = 0 \in \mathrm{GF}(2^p).$$

The assignment of values $\{y_{(c,v)}\}_{(c,v)\in E}$ that the edges convey is referred to as the *edge constellation*. We will count all the codewords of weight ℓ in all graphs in the ensemble $\mathcal{G}$ with k active edges, and sum them up for all $k \geq 0$.

Counting all these codewords involves the following 3 parts:

(i) Count the edge constellations satisfying all the parity-check constraints for k active edges.
(ii) Count the edge constellations which stem from codewords of symbol-weight ℓ and k active edges. In other words, such constellations have k active edges which incident to ℓ variable nodes.
(iii) Count the edge permutations among k active edges and $E-k$ non-active edges.

Before we start counting the edge constellations of (i), first, let us count the active edge constellations satisfying a single parity-check constraint. Consider a check node c of degree j. The check node c is satisfied if the j values that the connecting edges convey sum to 0, i.e., $\sum_{v\in V_c} y_{(c,v)} = 0$. Each symbol $y_{(c,v)}$ is in $\mathrm{GF}(2^p)$. Let $m_j(\ell)$ be the number of edge constellations that satisfy the single parity-check constraint. Equivalently, $m_j(\ell)$ is the number of sequences $(x_1,\ldots,x_j) \in \mathrm{GF}(2^p)^j$ such that

$$x_1 + \cdots + x_j = 0 \text{ and } |\{i \mid x_i \neq 0\}| = \ell.$$

It is obvious that $m_j(0) = 1, m_j(1) = 0$ and $m_j(2) = \binom{j}{2}(q-1)$. It is shown in [1, Eq. (5.3)] that

$$m_j(\ell) = \frac{(-1)^\ell(q-1)+(q-1)^\ell}{q}\binom{j}{\ell}.$$

The generating function of $m_j(\ell)$ is simply written as follows.

$$f_j(u) := \sum_{\ell=0}^{j} m_j(\ell)u^\ell = \frac{1}{q}\left((1+(q-1)u)^j + (q-1)(1-u)^j\right).$$

Next, count the edge constellations of (i). Since there are R_jN check nodes of degree j, the number of the edge constellations that satisfy all the M parity-check constraints with given k active edges is given by

$$\mathrm{coef}\left(\prod_{j=2}^{d_c} f_j(u)^{R_jN}, u^k\right). \tag{3}$$

Secondly, we will count the constellations of (ii), i.e., k active edges which stem from codewords of symbol-weight ℓ. Consider a variable node of degree i. Let $a(\ell,k)$ be the number of the constellations of k active edges which stem from a variable node v with a map $x_v \neq 0$ if $\ell = 1$ and $x_v = 0$ otherwise. From the definition of the active edges, it is easily checked that

$$a(\ell,k) = \begin{cases} 1 & (\ell = 0, k = 0), \\ 1 & (\ell = 1, k = i), \\ 0 & \text{otherwise.} \end{cases}$$

The generating function of $a(\ell,k)$ is given as follows.

$$\sum_{\ell\geq 0, k\geq 0} a(\ell,k)t^\ell s^k = 1 + ts^i.$$

Since there are L_iN variable nodes of degree i, the constellations of k active edges which stem from codewords of symbol-weight ℓ is given as

$$\mathrm{coef}\left(\prod_{i=2}^{d_v}(1+ts^i)^{L_iN}, t^\ell s^k\right). \tag{4}$$

Finally, we will count (iii), the edge permutations among k active edges and $E-k$ non-active edges. The number of possible ways of permuting active and non-active edges and assigning the values of active edges is given as

$$k!(E-k)!(q-1)^k \tag{5}$$

Let $A(\ell,k)$ be the average number of graphs which have codewords of symbol-weight ℓ for given k active edges. By multiplying Eqs. (3), (4) and (5), and dividing by the number of codes in the ensemble given in Eq. (2), we obtain

$$A(\ell,k) = \mathrm{coef}\left(\prod_{j=2}^{d_c} f_j(u)^{R_jN}, u^k\right) \mathrm{coef}\left(\prod_{i=2}^{d_v}(1+ts^i)^{L_iN}, t^\ell s^k\right) \Big/ \binom{E}{k}(q-1)^{E-k}.$$

The average number of codewords of symbol-weight ℓ for the ensemble is obtained by summing up $A(\ell, k)$ over the all possible active edge numbers.

$$A(\ell) = \sum_{k=0}^{E} A(\ell, k) \tag{6}$$

This concludes the proof. □

3.2 Bit-Weight Distribution for Non-binary LDPC Codes

In a similar way, we will derive the average bit-weight distribution of the non-binary irregular LDPC code ensemble $\mathcal{G}(N, \lambda(x), \rho(x), 2^p)$. First, consider a variable node of degree i. Let $a_{\mathrm{b}}(\ell, k)$ be the number of the constellations of k active edges which stem from a variable node v which has $\ell = 1$ in the binary representation of x_v. From the definition of the active edges, it is obvious that

$$a_{\mathrm{b}}(\ell, k) = \begin{cases} 1 & (\ell = 0, k = 0), \\ \binom{p}{\ell} & (\ell \geq 1, k = i), \\ 0 & \text{otherwise.} \end{cases}$$

The generating function of $a_{\mathrm{b}}(\ell, k)$ is given as follows.

$$\sum_{\ell \geq 0, k \geq 0} a(\ell, k) t^\ell s^k = 1 + ((1+t)^p - 1)s^i.$$

Since there are $L_i N$ variable nodes of degree i, the number of constellations of k active edges which stem from codewords of bit-weight ℓ is given as

$$\mathrm{coef}\left(\prod_{i=2}^{d_v} (1 + ((1+t)^p - 1)s^i)^{L_i N}, t^\ell s^k \right).$$

Using this, in a similar way as done for the symbol-weight distributions, the average number $A_{\mathrm{b}}(\ell)$ of codewords of bit-weight ℓ is given as follows.

Theorem 2: Let $n := pN$ be the bit-codelength. The average number $A_b(\ell)$ of codewords of bit-weight ℓ for the non-binary irregular LDPC code ensemble $\mathcal{G}(N = n/p, \lambda(x), \rho(x), 2^p)$ is given by

$$A_{\mathrm{b}}(\ell) = \sum_{k=0}^{E} A_{\mathrm{b}}(\ell, k), \tag{7}$$

$$A_{\mathrm{b}}(\ell, k) := \frac{\mathrm{coef}\left((Q_{\mathrm{b}}(s,t) P_{\mathrm{b}}(u))^n, t^\ell s^k u^k \right)}{\binom{E}{k}(q-1)^{E-k}},$$

$$Q_{\mathrm{b}}(s,t) := \prod_{i=2}^{d_v} (1 + ((1+t)^p - 1)s^i)^{L_i/p},$$

$$P_{\mathrm{b}}(u) := \prod_{j=2}^{d_c} f_j(u)^{R_j/p},$$

$$f_j(u) := \frac{1}{q}\left((1 + (q-1)u)^j + (q-1)(1-u)^j \right).$$

4. Asymptotic Analysis

In this section, we investigate the asymptotic behavior of the average weight distributions of non-binary LDPC code ensemble in the limit of large codelength. The number of codewords of fixed weight usually exponentially grows or decreases with codelength. We are interested in the rate of the exponential growth. We define

$$\gamma(\omega) := \lim_{N \to \infty} \frac{1}{N} \log_q A(\omega N),$$
$$\gamma_{\mathrm{b}}(\omega) := \lim_{n \to \infty} \frac{1}{n} \log A_{\mathrm{b}}(\omega n),$$

and refer to them as the *exponential growth rate* or simply *growth rate* of the average number of codewords in terms of symbol-weight and bit-weight, respectively. We use, unless otherwise specified, $\log(\cdot) = \log_2(\cdot)$.

With these growth rates, we can roughly estimate the number of codewords of symbol and bit-weight respectively by

$$A(\omega N) \sim q^{\gamma(\omega) N} \text{ and } A_{\mathrm{b}}(\omega n) \sim 2^{\gamma_{\mathrm{b}}(\omega) n},$$

where we denote $a_N \sim b_N$ if and only if $\lim_{N \to \infty} \frac{1}{N} \log_q \frac{a_N}{b_N} = 0$. For a fixed q, it can be seen that $a_n \sim b_n$ if and only if $\lim_{n \to \infty} \frac{1}{n} \log \frac{a_n}{b_n} = 0$, since $n = qN$.

We will investigate γ and γ_{b}. Since the techniques for deriving the growth rates of γ and γ_{b} are similar, we shall only provide the derivation for γ_{b}.

The number of terms in Eq. (7) is equal to $E + 1$, where E is defined in Eq. (1). Therefore, from Eq. (6) we have

$$\max_{k \geq 0} A_{\mathrm{b}}(\ell, k) \leq A_{\mathrm{b}}(\ell) \leq (E+1) \max_{k \geq 0} A_{\mathrm{b}}(\ell, k). \tag{8}$$

Therefore it follows that the largest term alone contributes the growth rate of $A_{\mathrm{b}}(\ell)$ as follows.

$$\frac{1}{n} \log A_{\mathrm{b}}(\ell) = \frac{1}{n} \log \max_{k \geq 0} A_{\mathrm{b}}(\ell, k) + o(1). \tag{9}$$

Rewrite $A_{\mathrm{b}}(\ell, k)$ as

$$A_{\mathrm{b}}(\omega n, \beta n) = \frac{\mathrm{coef}((Q_{\mathrm{b}}(s,t) P_{\mathrm{b}}(u))^n, (t^\omega s^\beta u^\beta)^n)}{\binom{\epsilon n}{\beta n}(q-1)^{(\epsilon - \beta)n}},$$

with

$$n = Np, \beta = k/n, \omega = \ell/n \text{ and } \epsilon = E/n.$$

We will calculate $\lim_{n \to \infty} \frac{1}{n} \log A_{\mathrm{b}}(\omega n, \beta n)$. In order to do this, we first introduce the following lemma.

Lemma 1 ([17], III.2): For an m-variable polynomial $g(x_1, \ldots, x_m)$ with non-negative coefficients, it holds that

$$\lim_{n \to \infty} \frac{1}{n} \log \mathrm{coef}(g(x_1, \ldots, x_m)^n, x_1^{\alpha_1 n} \cdots x_m^{\alpha_m n}) = \inf_{x_1, \ldots, x_m > 0} \log \frac{g(x_1, \ldots, x_m)}{x_1^{\alpha_1} \cdots x_m^{\alpha_m}}.$$

The point $(x_1, \ldots, x_m)$ that takes the minimum of

$$\frac{g(x_1, \ldots, x_m)}{x_1^{\alpha_1} \cdots x_m^{\alpha_m}}$$

is given by a solution of the following equations.

$$\frac{x_i}{g(x_1, \ldots, x_m)} \frac{\partial g(x_1, \ldots, x_m)}{\partial x_i} = \alpha_i \quad (i = 1, 2, \ldots, m)$$

Using Lemma 1 with (9), we obtain the following theorem.

Theorem 3: The growth rate $\gamma_{\mathrm{b}}(\omega)$ of the average number of codewords of normalized bit-weight ω for the non-binary irregular LDPC code ensemble $\mathcal{G}(N, \lambda(x), \rho(x), 2^p)$ is given by

$$\begin{aligned}\gamma_{\mathrm{b}}(\omega) &= \sup_{\beta>0} \inf_{t>0,s>,u>0} \Big[\log Q_{\mathrm{b}}(s,t) + \log P_{\mathrm{b}}(u) \\ &\quad - \beta \log(u) - \beta \log(s) - \omega \log(t) \\ &\quad - \epsilon h(\beta/\epsilon) - (\epsilon - \beta)\log(q-1)\Big] \\ &=: \sup_{\beta>0} \gamma_{\mathrm{b}}(\omega, \beta), \end{aligned} \tag{10}$$

where $h(x) := -x\log(x) - (1-x)\log(1-x)$. A point (u, s, t) that takes $\inf_{t,s,u}$ is given as a solution of the following equations.

$$\omega = t\frac{\frac{\partial Q_{\mathrm{b}}}{\partial t}}{Q_{\mathrm{b}}} = \sum_{i=2}^{d_v} \frac{L_i t(1+t)^{p-1} s^i}{1 + ((1+t)^p - 1)s^i}, \tag{11}$$

$$\beta = u\frac{\frac{\partial P_{\mathrm{b}}}{\partial u}}{P_{\mathrm{b}}} = u\sum_{j=2}^{d_c} \frac{R_j}{p} \frac{\frac{\partial f_j(u)}{\partial u}}{f_j(u)}, \tag{12}$$

$$= u\sum_{j=2}^{d_c} j(q-1)\frac{R_j}{p} \frac{(1+(q-1)u)^{j-1} - (1-u)^{j-1}}{(1+(q-1)u)^j + (q-1)(1-u)^j},$$

$$\beta = s\frac{\frac{\partial Q_{\mathrm{b}}}{\partial s}}{Q_{\mathrm{b}}} = \sum_{i=2}^{d_v} \frac{L_i}{p} \frac{i((1+t)^p - 1)s^i}{1 + ((1+t)^p - 1)s^i}. \tag{13}$$

A point β which gives the maximum of $\gamma_{\mathrm{b}}(\omega, \beta)$ needs to satisfy the stationary condition

$$-\log u - \log s - \log\frac{\epsilon - \beta}{\beta} + \log(q-1) = 0. \tag{14}$$

In a similar way, the growth rate $\gamma(\omega)$ of the average number of codewords of normalized symbol-weight ω is derived.

Note that, once the normalized weigh ω is fixed, the intermediate variables u, s, t and β can be viewed as functions of ω. Hereafter, we fix ω and denote u, s, t and β instead of $u(\omega)$, $s(\omega)$, $t(\omega)$ and $\beta(\omega)$.

In Theorem 3, the growth rate $\gamma_{\mathrm{b}}(\omega)$ seems too complicated to investigate the behavior of $\gamma_{\mathrm{b}}(\omega)$. Interestingly, the derivative of $\gamma_{\mathrm{b}}(\omega)$ in terms of ω can be expressed in the following simple form.

Lemma 2: For β and t such that $t \neq 0$ and Eqs. (11), (12) and (13) hold, we have

$$\frac{d}{d\omega}\gamma_{\mathrm{b}}(\omega) = -\log(t(\omega)).$$

Proof: Let x' denote the derivation of x with respect to ω. Differentiating $\gamma_{\mathrm{b}}(\omega)$ defined in Eq. (10), we have

$$\begin{aligned}\frac{d}{d\omega}\gamma_{\mathrm{b}}(\omega) &= \frac{Q'_{\mathrm{b}}}{Q_{\mathrm{b}}} + \frac{P'_{\mathrm{b}}}{P_{\mathrm{b}}} - w\frac{t'}{t} - \beta' \log\frac{\epsilon-\beta}{\beta} + \beta'\log(q-1) \\ &\quad - \log t - (\beta' \log u + \beta\frac{u'}{u} + \beta' \log s + \beta\frac{s'}{s}), \end{aligned} \tag{15}$$

where s is given by Eqs. (11), (12) and (13). Combining (12) and $P'_{\mathrm{b}} = \frac{\partial P_{\mathrm{b}}}{\partial u}u'$, we have

$$\frac{P'_{\mathrm{b}}}{P_{\mathrm{b}}} - \beta\frac{u'}{u} = 0 \tag{16}$$

From (11), (13) and $Q'_{\mathrm{b}} = \frac{\partial Q_{\mathrm{b}}}{\partial t}t' + \frac{\partial Q_{\mathrm{b}}}{\partial s}s'$, we have

$$\frac{Q'_{\mathrm{b}}}{Q_{\mathrm{b}}} - w\frac{t'}{t} + \beta\frac{s'}{s} = 0$$

Thus, substituting (14), we conclude the proof since the remaining term in the right hand side of (15) is $-\log t$. □

4.1 Analysis of Small Weight Codeword

In this section, we investigate how the number of codewords of small weight are changed by degree distribution pairs $(\lambda(x), \rho(x))$ and q. To this end, we analyze the growth rate $\gamma_{\mathrm{b}}(\omega)$ and $\gamma(\omega)$ for small normalized weight ω. From the linearity of LDPC codes, it follows that $A_{\mathrm{b}}(0) = 1$ and $\gamma_{\mathrm{b}}(0) = 0$. From (10) and Lemma 2, it holds that for $\omega \to 0$,

$$\gamma_{\mathrm{b}}(\omega) = \gamma'_{\mathrm{b}}(0)\omega + o(\omega) \tag{17}$$

$$= -\log(t)\omega + o(\omega), \tag{18}$$

where t is a t which satisfies (11), (12), (13) and (14) for $\omega \to 0$. From (11), for $\omega \to 0$, it holds that $t^j s^i \to 0$ for i such that $L_i \neq 0$ and $j = 1, \ldots, p$. Using this, we see that $\beta \to 0$ from (13). From Eq. (12), it is consequent that $u \to 0$. Moreover, from (12) it follows that as $u \to 0$,

$$\beta = \sum_{j=2}^{d_c} j(j-1)(q-1)\frac{R_j}{p}u^2 + o(u^2).$$

Substituting this to (14), we have

$$\begin{aligned}s &= \frac{1}{\epsilon}\sum_{j=2}^{d_c} j(j-1)\frac{R_j}{p}u + o(u) \\ &= \rho'(1)u + o(u). \end{aligned} \tag{19}$$

As $s \to 0$, from (13) we have

$$\beta = 2\frac{L_2}{p}((1+t)^p - 1)s^2 + o(s).$$

Substituting this to (14), we obtain the following.

$$u = \frac{2L_2}{\epsilon p(q-1)}((1+t)^p - 1)s + o(s) = \frac{\lambda'(0)}{q-1}((1+t)^p - 1)s + o(s). \quad (20)$$

From (19) and (20)

$$\lim_{\omega\to 0} \frac{\lambda'(0)\rho'(1)}{q-1}((1+t(\omega))^p - 1) = 1.$$

Therefore we have

$$\lim_{\omega\to 0} t(\omega) = \left(\left(\frac{q-1}{\lambda'(0)\rho'(1)} + 1\right)^{\frac{1}{p}} - 1\right).$$

In summary, we obtain the following theorem.

Theorem 4: For the non-binary irregular LDPC code ensemble $\mathcal{G}(N, \lambda(x), \rho(x), 2^p)$ with $\lambda'(0) > 0$, the growth rate $\gamma_{\rm b}(\omega)$ of the average number $A_{\rm b}(\omega n)$ of codewords of bit-weight ωn, in the limit of bit-codelength $n = pN$ for small ω, is given by

$$\gamma_{\rm b}(\omega) = -\log\left(\left(\frac{q-1}{\lambda'(0)\rho'(1)} + 1\right)^{\frac{1}{p}} - 1\right)\omega + O(\omega^2).$$

In a similar way, we have the following theorem.

Theorem 5: For the non-binary irregular LDPC code ensemble $\mathcal{G}(N, \lambda(x), \rho(x), 2^p)$ with $\lambda'(0) > 0$, the growth rate of the average number $A(\omega N)$ of codewords of symbol-weight ωN, in the limit of symbol-codelength N for small ω, is given by

$$\gamma(\omega) = -\log_q(\lambda'(0)\rho'(1))\omega + O(\omega^2).$$

The number of codewords of weight ωn is approximated by $A_{\rm b}(\omega n) \sim 2^{\gamma_{\rm b}(\omega)n}$. Therefore, if $\gamma_{\rm b}(\omega) < 0$ for small ω, there are exponentially few codewords of bit-weight ωn. It is important to know whether there are exponentially few or many codewords of small weight, since decoding errors in the large SNR region are due to the codewords of small weight. It can be seen from Theorem 4 that $\gamma'(0) < 0$ if and only if $\lambda'(0)\rho'(1) < 1$, which does not depend on the field size q. Furthermore, it can be seen from Theorem 5 that $\gamma'_{\rm b}(0) < 1$ if and only if $\lambda'(0)\rho'(1) < 1$. It makes sense that these conditions coincide.

In summary, we have the following corollary.

Corollary 1: For the non-binary irregular LDPC code ensemble $\mathcal{G}(N, \lambda(x), \rho(x), 2^p)$ and sufficiently large N, if $\lambda'(0)\rho'(1) < 1$, there exists $\delta > 0$ such that there are, in average, exponentially few codewords of bit-weight ωn for $\omega < \delta$.

We present some more facts on the growth rates.

Theorem 6: For the non-binary irregular LDPC code ensemble $\mathcal{G}(N, \lambda(x), \rho(x), 2^p)$, the growth rates for the full weight codewords, i.e., codewords of symbol-weight N and bit-weight n are given as follows.

$$\gamma(1) = \sum_{j=2}^{d_c} R_j \log_q\left((q-1)^j + (-1)^j(q-1)\right) - (1-r) - (p\epsilon - 1)\log_q(q-1) = r \quad (q\to\infty) \quad (21)$$

$$\gamma_{\rm b}(1) = \sum_{j=2}^{d_c} \frac{R_j}{p}\log\left((q-1)^j + (-1)^j(q-1)\right) - (1-r) - \epsilon\log(q-1) = r - 1 \quad (q\to\infty). \quad (22)$$

Codewords of symbol-weight $1 - 1/q$ and bit-weight $1/2$ alone consist of most of the code,

$$\gamma(1 - 1/q) = r, \quad \gamma_{\rm b}(1/2) = r. \quad (23)$$

In other words, $A((1-1/q)N) \sim q^{rN}$ and $A_{\rm b}(n/2) \sim 2^{rn}$.

Proof: Since the proofs are almost the same for the growth rate for both symbol and bit-weight, we focus on the proofs for Eqs. (22) and (23). Substitute $\ell = n$ in Eq. (7) we have

$$A_{\rm b}(n) = \frac{\prod_{j=2}^{d_c}\left((q-1)^j + (-1)^j(q-1)\right)^{R_j n/p}}{q^{(1-r)n/p}(q-1)^{\epsilon n}}, \quad (24)$$

which concludes Eq. (22). It can be seen that

$$(\omega, \beta, s, t, u) = \left(\frac{1}{2}, \epsilon\frac{q-1}{q}, 1, 1, 1\right)$$

satisfies Eqs. (11), (12), (13), (14). Substituting this to Eq. (10), we have Eq. (23). □

5. Numerical Examples

In this section, we demonstrate Theorem 3. We choose the degree distribution pair as $(\lambda(x) = \frac{1}{7}x + \frac{6}{7}x^2, \rho(x) = x^3)$ with $\lambda'(0)\rho'(1) = 3/7$ and design rate $r = 0.3$.

Figures 1 and 2 show the growth rate for the average symbol-weight distributions of the irregular LDPC code ensembles defined over GF($q = 2^p$) for $p = 1, 2, \ldots, 9$. As expected in Eq. (21), $\gamma_{\rm b}(1)$ for $p = 1, \ldots, 9$ converge to $r = 0.3$ and attain $r = 0.3$ at $\omega = 1 - 1/q$.

Figures 3 and 4 show the growth rate for the average bit-weight distributions of the ensembles. As expected in Eq. (22), $\gamma_{\rm b}(1)$ rapidly converges to $r - 1 = -0.7$. Indeed $\gamma_{\rm b}(1) = 0.0000$, -0.6816, -0.6990, and -0.6999 for p =1, 2, 3 and 4, respectively. Moreover, it can be seen that the curves at $\omega > 1/2$ rapidly converge to the growth rate of the binary random code ensemble of rate r.

Each curve for bit and symbol-weight takes negative values for small normalized bit-weight (resp. symbol-weight) ω. We call the minimum normalized bit-weight (resp. symbol-weight) crossing with 0 as *normalized typical minimum distance* τ, since there are exponentially few codewords of bit-weight ωn (resp. resp. symbol-weight ωN) for

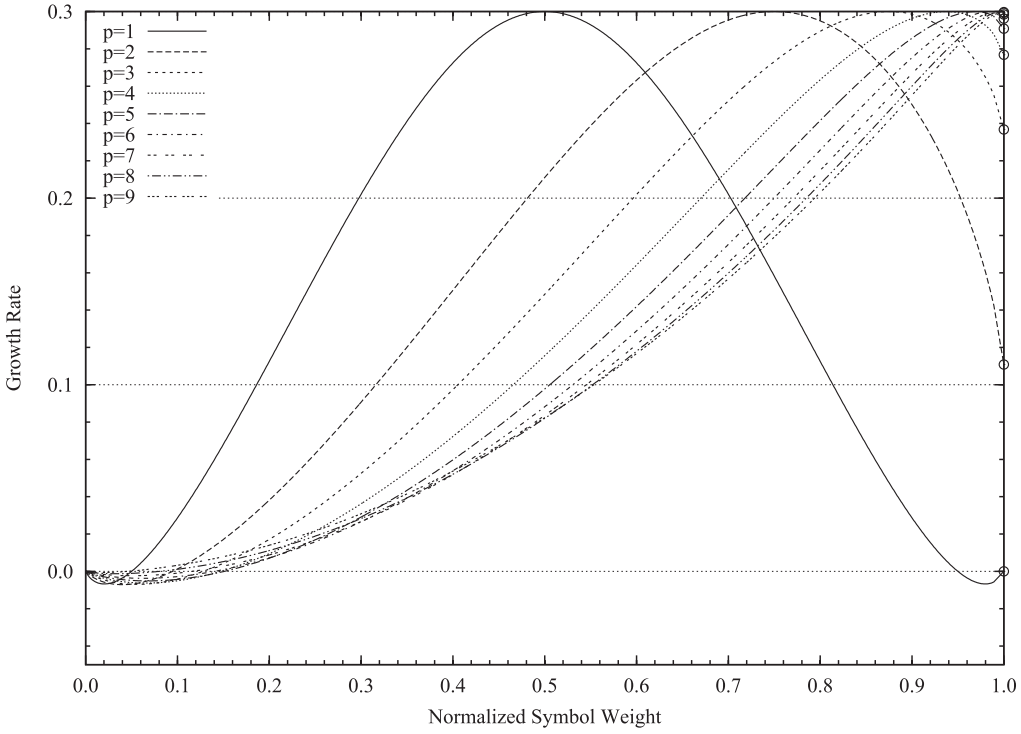

Fig. 1 The growth rate of the average symbol-weight distributions of a $(\lambda(x) = \frac{1}{7}x + \frac{6}{7}x^2, \rho(x) = x^3)$-irregular LDPC code ensemble defined over GF(q), The rate is $r = 0.3$. The endpoints at $\omega = 1$ are plotted with circles.

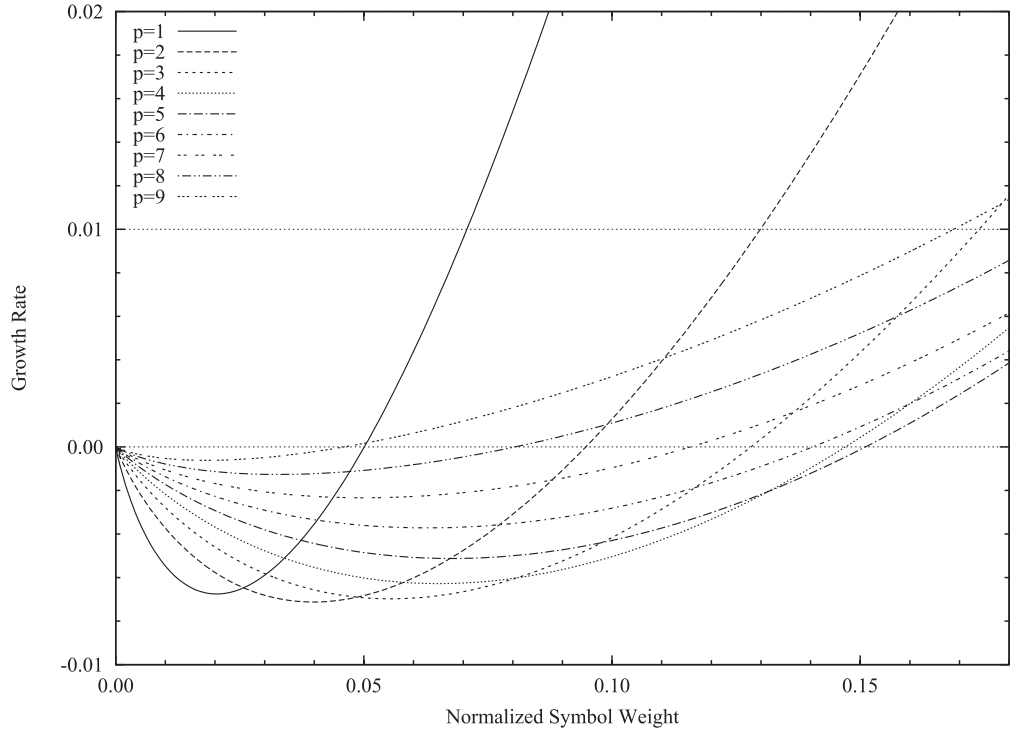

Fig. 2 The growth rate of the average symbol-weight distributions of a $(\lambda(x) = \frac{1}{7}x + \frac{6}{7}x^2, \rho(x) = x^3)$-irregular LDPC code ensemble defined over GF(q), The rate is $r = 0.3$.

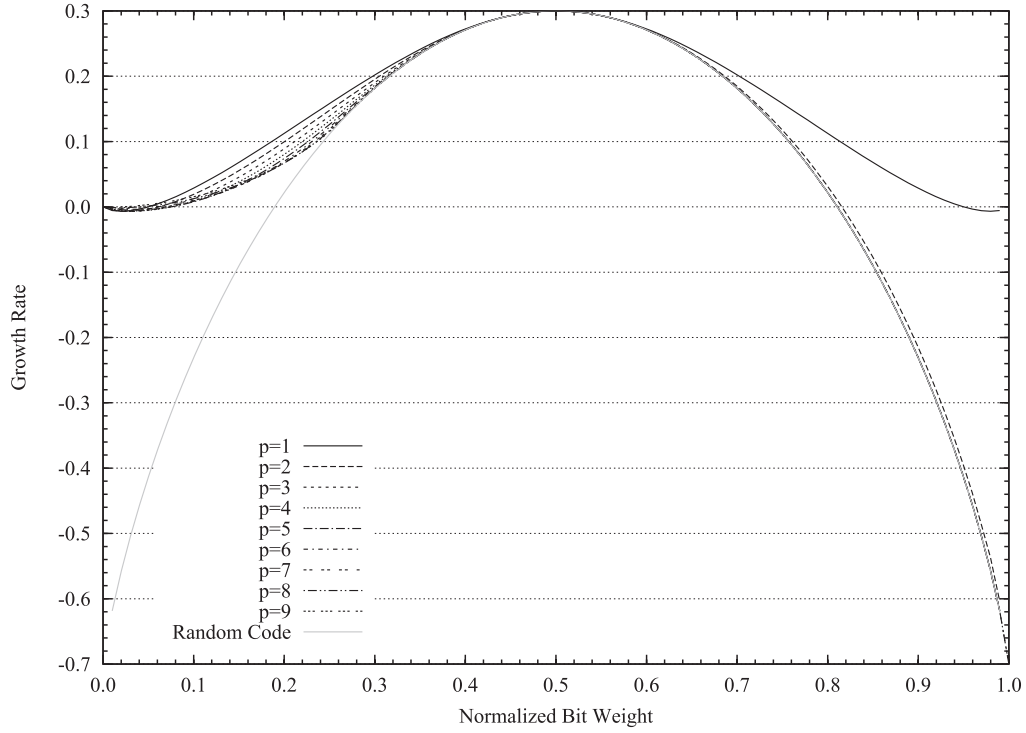

Fig. 3 The growth rate of the average bit-weight distributions of a $(\lambda(x) = \frac{1}{7}x + \frac{6}{7}x^2, \rho(x) = x^3)$-irregular LDPC code ensemble defined over GF(q), The rate is $r = 0.3$.

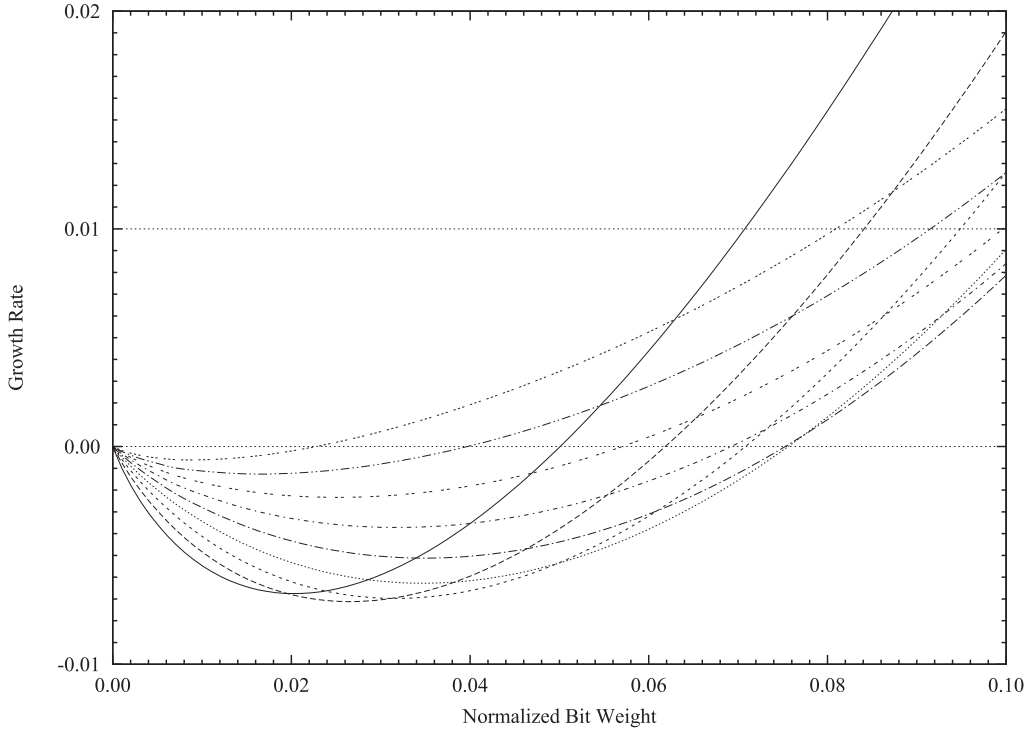

Fig. 4 The growth rate of the average bit-weight distributions of a $(\lambda(x) = \frac{1}{7}x + \frac{6}{7}x^2, \rho(x) = x^3)$-irregular LDPC code ensemble defined over GF(q), The rate is $r = 0.3$.

$\omega < \tau$.

Interestingly, the normalized typical minimum distance does not monotonically grow with q. It grows monotonically for small q and then starts decreasing for large q. In other words, there exists a field size which locally maximizes the normalized typical minimum distance. The local maximum size is attained at $q = 2^5$ for symbol-weight and $q = 2^4$ for bit-weight.

6. Conclusion

In this paper, we derived the weight distributions of non-binary LDPC codes. The analysis of the exponential growth rate of the weight distributions revealed that the number of codewords of small normalized weight grows (reps. vanishes) exponentially with the codelength iff $\lambda'(0)\rho'(1)$ is greater (resp. less) than 1. Moreover, we observed the non-monotonicity of the field size for the normalized typical minimum distance.

Another non-monotonicity of the field size was observed for the thresholds of BP decoding. Rathi showed that the threshold is not monotonic with the field size [22, Table 1]. The field sizes for the local optimal typical minimum distance and threshold do not coincide. We expect some relation between these two monotonousness.

References

[1] R.G. Gallager, Low Density Parity Check Codes, in Research Monograph series, MIT Press, Cambridge, 1963.
[2] F. Kschischang, B. Frey, and H.A. Loeliger, "Factor graphs and the sum-product algorithm," IEEE Trans. Inf. Theory, vol.47, no.2, pp.498–519, Feb. 2001.
[3] T. Richardson and R. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," IEEE Trans. Inf. Theory, vol.47, no.2, pp.599–618, Feb. 2001.
[4] T.J. Richardson, M.A. Shokrollahi, and R.L. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," IEEE Trans. Inf. Theory, vol.47, no.2, pp.619–637, Feb. 2001.
[5] M. Davey and D. MacKay, "Low-density parity check codes over GF(q)," IEEE Commun. Lett., vol.2, no.6, pp.165–167, June 1998.
[6] W. Chang and J. Cruz, "Nonbinary LDPC codes for 4-kB sectors," IEEE Trans. Magn., vol.44, no.11, pp.3781–3784, Nov. 2008.
[7] I. Djordjevic and B. Vasic, "Nonbinary LDPC codes for optical communication systems," IEEE Photonics Technol. Lett., vol.17, no.10, pp.2224–2226, Oct. 2005.
[8] B. Zhou, J. Kang, S. Song, S. Lin, K. Abdel-Ghaffar, and M. Xu, "Construction of non-binary quasi-cyclic LDPC codes by arrays and array dispersions," IEEE Trans. Commun., vol.57, no.6, pp.1652–1662, June 2009.
[9] M. Arabaci, I. Djordjevic, R. Saunders, and R. Marcoccia, "High-rate nonbinary regular quasi-cyclic LDPC codes for optical communications," J. Lightwave Technol., vol.27, no.23, pp.5261–5267, Dec. 2009.
[10] B. Zhou, J. Kang, Y. Tai, S. Lin, and Z. Ding, "High performance non-binary quasi-cyclic LDPC codes on euclidean geometries LDPC codes on euclidean geometries," IEEE Trans. Commun., vol.57, no.5, pp.1298–1311, May 2009.
[11] D. Declercq and M. Fossorier, "Decoding algorithms for nonbinary LDPC codes over GF(q)," IEEE Trans. Commun., vol.55, no.4, pp.633–643, April 2007.
[12] K. Kasai, Y. Fujisaka, and M. Onsjö, "FFT-based parallel decoder of non-binary LDPC codes on GPU: KFO_NBLDPC_GPU," 2009.
[13] G. Miller and D. Burshtein, "Bounds on the maximum-likelihood decoding error probability of low-density parity-check codes," IEEE Trans. Inf. Theory, vol.47, no.7, pp.2696–2710, Nov. 2001.
[14] C. Di, T. Richardson, and R. Urbanke, "Weight distribution of low-density parity-check codes," IEEE Trans. Inf. Theory, vol.52, no.11, pp.4839–4855, Nov. 2006.
[15] A. Orlitsky, K. Viswanathan, and J. Zhang, "Stopping set distribution of LDPC code ensembles," IEEE Trans. Inf. Theory, vol.51, no.3, pp.929–953, March 2005.
[16] S. Litsyn and V. Shevelev, "On ensembles of low-density parity-check codes: Asymptotic distance distributions," IEEE Trans. Inf. Theory, vol.48, no.4, pp.887–908, April 2002.
[17] D. Burshtein and G. Miller, "Asymptotic enumeration methods for analyzing LDPC codes," IEEE Trans. Inf. Theory, vol.50, no.6, pp.1115–1131, June 2004.
[18] T. Richardson and R. Urbanke, Modern Coding Theory, Cambridge University Press, 2008.
[19] K. Kasai, T. Awano, C. Poulliat, D. Declercq, and K. Sakaniwa, "Weight distributions of multi-edge type LDPC codes," IEICE Trans. Fundamentals, vol.E93-A, no.11, pp.1942–1948, Nov. 2010.
[20] X.Y. Hu, Low-delay low-complexity error-correcting codes on sparse graphs, Ph.D. Thesis, Ecole Polytechnique Federale de Lausanne (EPFL), 2003.
[21] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, Elsevier, Amsterdam, 1977.
[22] V. Rathi and R. Urbanke, "Density evolution, threshold and the stability condition for non-binary LDPC codes," IEE Proc. Commun., vol.152, no.6, pp.1069–1074, 2005.

Kenta Kasai received B.E., M.E. and Ph.D. degrees from Tokyo Institute of Technology in 2001, 2003 and 2006, respectively. Since April 2006, he has been an assistant professor in the Department of Communications and Integrated Systems, Graduate School of Science and Engineering, Tokyo Institute of Technology. His current research interests include codes on graphs and iterative decoding algorithms.

Charly Poulliat received the E.E. degree from the Ecole Nationale Supérieure de I' Electronique et de ses Applications (ENSEA), Cergy-Pontoise, France, and the M.S. degree in Image and Signal Processing from the University of Cergy-Pontoise, France, both in 2001, and his Ph.D. degree in Electrical and Computer Engineering from the University of Cergy-Pontoise, France, in 2004. From November 2004 to October 2005, he was a post-doctoral researcher at UH coding group supervised by Pr. Marc Fossorier, University of Hawaii at Manoa, HI, USA. He is currently an assistant professor at the ENSEA, and teaches digital signal processing and communication theory. He is a member of the ETIS-CNRS Laboratory in Cergy-Pontoise, France. His research interests include channel coding and information theory, iterative system design and optimization, unequal error protection techniques (UEP), joint source and channel coding/decoding, signal processing for digital communications.

David Declercq received his Ph.D. degree in electrical and computer engineering in 1998 from the university of Cergy-Pontoise, France. He was a visiting junior researcher in 1999 in the university of Minneapolis, USA. In 2000, he joined the "Ecole Normale Supérieure de I' Electronique et de ses Applications" (ENSEA), a graduate school in electrical and computer engineering, where he is now a full professor. He is associated with the ETIS ENSEA/univ. Cergy-Pontoise/CNRS UMR8051 Laboratory in Cergy-Pontoise, France, and led the signal processing research group from 2003 to 2006. He was head of the research department at the ENSEA from 2007 to 2009. He is since 2006 scientific director of the French research network CNRS-GdR-ISIS, and secretary of the image/signal processing GRETSI association. His research interests are mainly statistical model estimation and coding theory for digital communication. In particular, he is interested in the design of efficient binary and non-binary LDPC codes and in decoder complexity reduction. He participated in the FP6-STREP M-PIPE project, the FP6/FP7 NewCom Network of Excellence, and was leader of the FP7-STREP DaVinci project. He was awarded the Junior Position of the "Institut Universitaire de France" in 2009.

Kohichi Sakaniwa received B.E., M.E., and Ph.D. degrees all in electronic engineering from the Tokyo Institute of Technology, Tokyo Japan, in 1972, 1974 and 1977, respectively. He joined the Tokyo Institute of Technology in 1977 as a research associate and served as an associate professor from 1983 to 1991. Since 1991 he has been a professor in the Department of Electrical and Electronic Engineering, and since 2000 in the Department of Communication and Integrated Systems, Graduate School of Science and Engineering, both in the Tokyo Inst. of Tech. From November 1987 to July 1988, he stayed at the University of Southwestern Louisiana as a Visiting Professor. He received the Excellent Paper Award from the IEICE of Japan in 1982, 1990, 1992 and 1994. His research area includes Communication Theory, Error Correcting Coding, (Adaptive) Digital Signal Processing and so on. Dr. Sakaniwa is a member of IEEE, Information Processing Society of Japan, Institute of Image Information and Television Engineers of Japan, and Society of Information Theory and its Applications.