Multiplicatively Repeated Non-Binary LDPC Codes

Kenta Kasai, David Declercq, Charly Poulliat, Kohichi Sakaniwa

Multiplicatively Repeated Nonbinary LDPC Codes

Kenta Kasai, *Member, IEEE*, David Declercq, *Member, IEEE*, Charly Poulliat, *Member, IEEE*, and Kohichi Sakaniwa, *Senior Member, IEEE*

***Abstract*—We propose nonbinary LDPC codes concatenated with multiplicative repetition codes. By multiplicatively repeating the (2,3)-regular nonbinary LDPC mother code of rate 1/3, we construct rate-compatible codes of lower rates $1/6, 1/9, 1/12, \ldots$. Surprisingly, such simple low-rate nonbinary LDPC codes outperform the best low-rate binary LDPC codes so far. Moreover, we propose the decoding algorithm for the proposed codes, which can be decoded with almost the same computational complexity as that of the mother code.**

***Index Terms*—Iterative decoding, low-rate code, nonbinary low-density parity-check code, rate compatible code, repetition code.**

I. Introduction

In 1963, Gallager invented low-density parity-check (LDPC) codes [2]. Due to sparsity of the code representation, LDPC codes are efficiently decoded by belief propagation (BP) decoders. By a powerful optimization method *density evolution* [3], developed by Richardson and Urbanke, messages of BP decoding can be statistically evaluated. The optimized LDPC codes can approach very close to Shannon limit [4].

Rate-adaptability is a desirable property of coding systems. Over time-varying channels, the system adapts the coding rate according to the quality of the channels. Using the different type of codes for different rates results in a complex coding system. It is desirable to use a single encoder and decoder pair compatible with different rates. Such a property of codes is referred to as rate-compatibility. Moreover, rate-compatible codes allow us to transmit bits gradually in conjunction with automatic repeat request (ARQ). By puncturing a low rate code, we can construct rate-compatible codes of higher rates.

In order to reliably transmit information over the very noisy communication channels, one needs to encode the information at low coding rate. As described in [5], one encounters a difficulty when designing low-rate LDPC codes, while for high rate codes, even binary regular LDPC codes have good thresholds. The optimized low-rate structured LDPC codes, e.g., accumulate repeat accumulate (ARA) code [6, Table 1] of rate 1/6 and multiedge type LDPC code [5, Table X] of rate 1/10 have good thresholds. However, the maximum row-weights of those codes are as high as 11 and 28, respectively. Such high row weights lead to dense parity-check matrices and degraded performance for short code length. We note that, with very large code length, generalized LDPC codes with Hadamard codes [7] perform very close to the ultimate Shannon limit [8]. However, the large code length leads to transmission latency. If two error correcting codes with the same error-correcting capabilities and different code length are given, the shorter code is preferred.

Another obstacle blocking the realization of the low-rate LDPC codes is the large number of check node computations. For a fixed information length K, it can be easily seen that the number M of check nodes gets larger as the coding rate R gets lower. To be precise, $M = K(1-R)/R$. In the BP decoding, computations of check nodes are usually more complex than those of variable nodes. It is a desirable property for the low-rate LDPC codes to be decoded with computational complexity comparable to that of the higher-rate LDPC codes.

The problems for constructing low-rate LDPC codes are summarized as follows.

- **Problem 1**: The Tanner graphs of low-rate LDPC codes tend to have many check nodes that require more complex computations than variable nodes.
- **Problem 2**: The Tanner graphs of optimized low-rate LDPC codes tend to have check nodes of high degree, which results in the degraded decoding performance for small code length.
- **Problem 3**: The optimized low-rate LDPC codes need to be used with large code length to exploit the potential decoding performance.

In this paper, we deal with all these issues.

In this paper, we consider nonbinary LDPC codes defined by sparse parity-check matrices over GF(2^m) for $2^m > 2$. Nonbinary LDPC codes were invented by Gallager [2]. Davey and MacKay [9] found nonbinary LDPC codes can outperform binary ones. Nonbinary LDPC codes have captured much attention recently due to their decoding performance [10]–[14].

It is known that irregularity of Tanner graphs help improve the decoding performance of binary LDPC codes [4], while it is not the case for the nonbinary LDPC codes. The $(2, k)$-regular nonbinary LDPC codes over GF(2^m) are empirically known [15] as the best performing codes for $2^m \geq 64$, especially for short code length. This means that, for designing nonbinary LDPC codes, one does not need to optimize the degree distributions of Tanner graphs, since $(2, k)$-regular nonbinary LDPC codes are best. Furthermore, sparsity of $(2, k)$-regular Tanner graph helps efficient decoding.

Sassatelli *et al.* proposed hybrid nonbinary LDPC codes [16] whose symbols are defined over the Galois fields of different sizes, e.g., over GF(2), GF(8), and GF(16) and whose Tanner

Manuscript received April 27, 2010; revised November 26, 2010; accepted April 26, 2011. Date of current version October 07, 2011. The material in this paper was presented in part at the IEEE International Symposium on Information Theory (ISIT), Austin, TX, June 2010.

K. Kasai and K. Sakaniwa are with the Department of Communications and Integrated Systems, Graduate School of Science and Engineering, Tokyo Institute of Technology, Tokyo 152-8550, Japan (e-mail: kenta@comm.ss.titech.ac.jp; sakaniwa@comm.ss.titech.ac.jp).

D. Declercq and C. Poulliat are with the ETIS Laboratory, UMR8051 ENSEA UCP CNRS, 95014 Cergy-Pontoise, France (e-mail: declercq@ensea.fr; poulliat@ensea.fr).

Communicated by I. Sason, Associate Editor for Coding Theory.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2011.2162259

graphs are irregular. In other words, the codes have two types of irregularity, i.e., irregularity of the degree distributions of graphs and the size distributions of Galois fields. To the best of the authors' knowledge, the decoding performance of the hybrid nonbinary LDPC codes are best so far among the low-rate codes of short code length.

In this paper, we investigate nonbinary LDPC codes concatenated with multiplicative repetition inner codes. We use a (2, 3)-regular nonbinary LDPC code of rate 1/3, as a mother code. By multiplicatively repeating the mother code, we construct codes of lower rates $1/6, 1/9, 1/12, \ldots$. Furthermore, we present a decoding algorithm for the proposed codes. And we show the computational complexity of decoding is almost the same as that of the mother code. The codes exhibit surprisingly better decoding performance than the best codes so far for small and moderate code length.

The rest of this paper is organized as follows. Section II defines the proposed codes. Section III describes the decoding algorithm for the proposed codes. In Section IV, we investigate the thresholds for the proposed codes transmitted over the binary erasure channels (BEC) by *density evolution* [4], [17]. In Section V, for the BEC and AWGN channels, we compare the decoding performance of the proposed codes and the best known codes for short and moderate code length.

II. Concatenation of Nonbinary LDPC Codes and Multiplicative Repetition Codes

We deal with elements of GF(2^m) as nonbinary symbols. For transmitting over the binary input channels, each nonbinary symbol in GF(2^m) needs to be represented by a binary sequence of length m. For each m, we fix a Galois field GF(2^m) with a primitive element α and its primitive polynomial π. Once a primitive element α of GF(2^m) is fixed, each symbol is given a m-bit representation [18, pp. 110]. For example, with a primitive element $\alpha \in$ GF(2^3) such that $\pi(\alpha) = \alpha^3 + \alpha + 1 = 0$, 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 $\alpha^6 = (1,0,1)$.

A nonbinary LDPC code C over GF(2^m) is defined by the null space of a sparse $M \times N$ parity-check matrix $H = \{h_{ij}\}$ defined over GF(2^m)

$$C = \{x \in \text{GF}(2^m)^N \mid Hx = 0 \in \text{GF}(2^m)^M\}.$$

The cth parity-check equation for $c = 1, \ldots, M$ is written as

$$h_{c1}x_1 + \cdots + h_{cN}x_N = 0 \in \text{GF}(2^m),$$

where $h_{c1}, \ldots, h_{cN} \in$ GF(2^m) and $x_1, \ldots, x_N \in$ GF(2^m).

Binary LDPC codes are represented by Tanner graphs with variable and check nodes [19, pp. 75]. The nonbinary LDPC codes, in this paper, are also represented by bipartite graphs with variable nodes and check nodes, which are also referred to as Tanner graphs. For a given sparse parity-check matrix $H = \{h_{cv}\}$ over GF(2^m), the graph is defined as follows. The vth variable node and cth check node are connected if $h_{cv} \neq 0$. By $v = 1, \ldots, N$ and $c = 1, \ldots, M$, we also denote the vth variable node and cth check node, respectively.

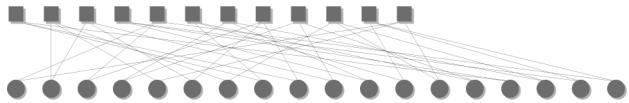

Fig. 1. An example of a mother code C_1. A nonbinary (2,3)-regular LDPC code of rate 1/3 over GF(2^m). Each variable node represents a symbol in GF(2^m). Each check node represents a parity-check equation over GF(2^m). The code length is 18 symbols in GF(2^m) or equivalently 18 m bits. Circle and square nodes represent variable and check nodes, respectively. The lower-rate codes C_T for $T = 2, 3 \ldots$ are constructed from C_1.

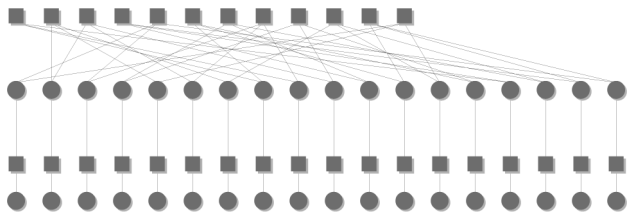

Fig. 2. An example of C_2. A nonbinary (2,3)-regular LDPC code over GF(2^m) concatenated with inner multiplicative repetition codes of length 2. The code length is 36 symbols or equivalently 36 m bits. The rate is 1/6.

A nonbinary LDPC code with a parity-check matrix over GF(2^m) is called (d_v, d_c)-regular if all the columns and all the rows of the parity-check matrix have weight d_v and d_c, respectively, or equivalently all the variable and check nodes have degree d_v and d_c, respectively.

Let C_1 be a (2,3)-regular LDPC code defined over GF(2^m) of length N symbols or equivalently mN bits and of rate 1/3. The code C_1 has a $2N/3 \times N$ sparse parity-check matrix H over GF(2^m). The matrix H has row weight 3 and column weight 2. Fig. 1 shows the Tanner graph of an example C_1 of length $N = 18$ symbols.

By using C_1 as a mother code, we will construct codes $C_2, C_3, \ldots, C_T$ of lower rates in the following way. Choose N coefficients $r_{N+1}, \ldots, r_{2N}$ uniformly at random from GF(2^m) $\setminus \{0\}$. The lower-rate code C_2 is constructed as follows:

$$C_2 = \{(x_1, \ldots, x_{2N}) | x_{N+v} = r_{N+v}x_v, \text{ for } v = 1, \ldots, N, (x_1, \ldots, x_N) \in C_1\}.$$

Since the resulting code C_2 has code length $2N$ and the same number of codewords as C_1, then the rate is 1/6. Fig. 2 shows the Tanner graph of C_2 of length $2N = 36$ symbols. We say that $x_{N+v} = r_{N+v}x_v$ is a *multiplicative repetition* symbol of x_v for $v = 1, \ldots, N$. Each variable node of degree one in Fig. 2 represents a multiplicative repetition symbol x_{N+v} for $v = 1, \ldots, N$. And each check node of degree two in Fig. 2 represents a parity-check constraint $x_{N+v} + r_{N+v}x_v = 0$ for $v = 1, \ldots, N$.

For $T \geq 3$, in a recursive fashion, by choosing N coefficients $r_{(T-1)N+1}, \ldots, r_{TN}$ randomly chosen from GF(2^m) $\setminus \{0\}$, the further low-rate code C_T is constructed from C_{T-1} as follows.

$$C_T = \{(x_1, \ldots, x_{TN}) | x_{(T-1)N+v} = r_{(T-1)N+v}x_v, \text{ for } v = 1, \ldots, N, (x_1, \ldots, x_{(T-1)N}) \in C_{T-1}\}.$$

The code C_T has length TN and rate $1/(3T)$. Fig. 3 shows the Tanner graph of C_3 of $3N = 54$ symbol code length. Fig. 4

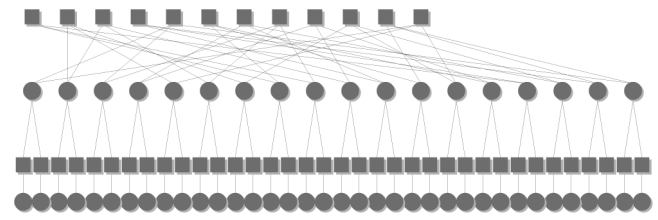

Fig. 3. An example of C_3. A nonbinary (2,3)-regular LDPC code over GF(2^m) concatenated with one inner multiplicative repetition codes of length 3. The code length is 54 symbols or equivalently 54 m bits. The rate is 1/9.

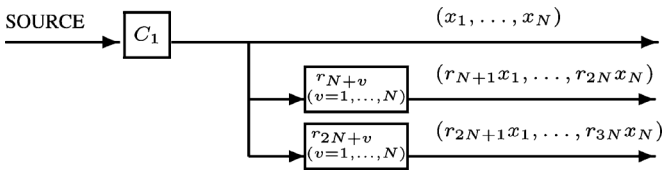

Fig. 4. The block diagram of the encoder of C_3. First, source of $N/3$ symbols in GF(2^m) are encoded with a (2,3)-regular LDPC code C_1 over GF(2^m). Next, each symbol in the codeword x_v, for $v = 1, \ldots, N$, is randomly multiplied by r_{N+v} and r_{2N+v} from GF(2^m) $\setminus \{0\}$ to generate x_{N+v} and x_{2N+v}.

shows the block diagram of the encoding of C_3. We refer to T as the repetition parameter.

Concatenating a binary code with repetition codes is known as the worst coding scheme. Indeed, repeating a binary code just doubles the number of channel use without any improvement of the curve of the decoding error rate v.s. $\mathrm{E_b/N_0}$. Note that the proposed code C_T are not generated by simple repetitions of the mother code but the random multiplicative repetitions of nonbinary symbols. Since the coefficient $r_{N+v}, \ldots, r_{(T-1)N+v}, \in$ GF(2^m) $\setminus \{0\}$ is randomly chosen, the multiplicative repetition $x_v \mapsto (x_v, r_{N+v}x_v, \ldots, r_{(T-1)N+v}x_v,)$ can be viewed as a random code of length mT bits. In other words, the proposed codes can be viewed as nonbinary LDPC codes over GF(2^m) serially concatenated with N random binary codes of length mT. Intuitively, this explains why multiplicative repetition works better than simple repetition.

The construction of the proposed codes may remind some readers of Justesen codes [20]. Note that the proposed construction chooses the multiplicative coefficients uniformly at random. Note also that since the minimum distance of C_1 is at most $O(\log(N))$ [15], the C_T code has minimum distance is at most $O(T \log(N))$.

Due to the repetition of symbols, the encoder are inherently rate-compatible.

III. Decoding Scheme

The BP decoder for nonbinary LDPC codes [21] exchanges probability vectors of length 2^m, called *messages*, between variable nodes and check nodes, at each iteration round $\ell \geq 0$. The proposed codes C_T for $T \geq 2$ also can be decoded by the BP decoding algorithm on the Tanner graphs of C_T. In this section, instead of the immediate use of the BP decoding on the Tanner graph of C_T, we propose a decoding algorithm which uses only the Tanner graph of C_1 for decoding C_T for $T \geq 2$.

The variable nodes of degree one in Figs. 2 and 3 represent multiplicative repetition symbols of C_2 and C_3, respectively. If the BP decoding algorithm is immediately applied to the proposed codes, all the variable nodes and check nodes, including the variable nodes of those multiplicative repetition symbols, are activated, i.e., exchage the messages. However, the messages reaching the variable nodes of degree one do not change messages that are sent back from the nodes. Therefore, the decoder does not need to pass the messages all the way to those variable nodes of degree 1 and their adjacent check nodes of degree 2. Consequently, after the variable nodes of degree 1 pass the initial messages to the upper part of the graph, the decoder uses only the upper part of the graph, i.e., C_1.

The computations of check nodes are more complex than those of variable nodes. As posed in Section I, Problem 1, the number M of the check nodes gets higher as R decreases. In general, LDPC codes of information length K and rate R have $K(1-R)/R$ check nodes. In our setting, we have $K = N/3$ information symbols. The number of check nodes in the proposed code C_T for $T \geq 2$ is also given by $K(1-R)/R$. However, $(T-1)N$ check nodes of degree 2 adjacent to the $(T-1)N$ variable nodes of degree 1 do not need to participate in the BP decoding iterations. The only $2N/3$ active check nodes in the mother code C_1 participate in the BP decoding algorithm for decoding C_T for $T \geq 2$. Note that the number of active check nodes $2N/3$ remains unchanged for any $T \geq 1$. This is highly preferable property for low-rate LDPC codes, which relieves Problem 1. Problem 2 is also relieved, since the maximum degree of check nodes in the mother code C_1 is as small as 3.

The BP decoding involves mainly 4 parts, i.e., the initialization, the check to variable computation, the variable to check computation, and the tentative decision parts. For $v = 1, \ldots, NT$, let X_v be the random variables with realizations x_v. Let Y_v be the random variables with realizations y_v which is received value from the channel $\Pr(Y_v|X_v)$ and the probability of transmitted symbol $\Pr(X_v)$ is assumed to be uniform.

We assume the decoder knows the channel transition probability

$$\Pr(X_v = x|Y_v = y_v), v = 1, \ldots, NT \tag{1}$$

for $x \in$ GF(2^m). When the transmissions take place over the memoryless binary-input output-symmetric channels, we can rewrite (1) as

$$\Pr(X_v = x|Y_v = y_v) = \prod_{i=1}^{m} \Pr(X_{v,i} = x_i|Y_{v,i} = y_{v,i}),$$

where $(x_1, \ldots, x_m) \in$ GF$(2)^m$ is the binary representation of $x \in$ GF(2^m) and $X_{v,i}$ is the random variable of the transmitted bit, and the corresponding channel output $y_{v,i}$ and its random variable $Y_{v,i}$.

A. Decoding Algorithm

Initialization: For each variable node v in C_1 for $v = 1, \ldots, N$, compute $p_v^{(0)}(x)$ as follows:

$$p_v^{(0)}(x) = \xi \Pr(X_v = x|Y_v = y_v) \prod_{t=1}^{T-1} \Pr(X_{tN+v} = r_{tN+v}x|Y_{tN+v} = y_{tN+v}), \tag{2}$$

for $x \in \mathrm{GF}(2^m)$, where ξ is the normalization factor so that $\sum_{x\in\mathrm{GF}(2^m)} p_v^{(0)}(x) = 1$. Each variable node $v = 1, \ldots, N$ in C_1 sends the initial message $p_{vc}^{(0)} = p_v^{(0)} \in \mathbb{R}^{2^m}$ to each adjacent check node c. Set the iteration round as $\ell{:=}0$.

Check to Variable: For each check node $c = 1, \ldots, M$ in C_1, let ∂c be the set of the adjacent variable nodes of c. It holds that $\#\partial c = 3$, since the mother code C_1 is (2,3)-regular. Each c has 3 incoming messages $p_{vc}^{(\ell)}$ for $v \in \partial c$ from the 3 adjacent variable nodes. The check node c sends the following message $p_{cv}^{(\ell+1)} \in \mathbb{R}^{2^m}$ to each adjacent variable node $v \in \partial c$:

$$\begin{aligned}
&\tilde{p}_{vc}^{(\ell)}(x) = p_{vc}^{(\ell)}(h_{cv}^{-1}x) \text{ for } x \in \mathrm{GF}(2^m),\\
&\tilde{p}_{cv}^{(\ell+1)} = \otimes_{v'\in\partial c\setminus\{v\}} \tilde{p}_{v'c}^{(\ell)},\\
&p_{cv}^{(\ell+1)}(x) = \tilde{p}_{cv}^{(\ell+1)}(h_{cv}x) \text{ for } x \in \mathrm{GF}(2^m).
\end{aligned}$$

where $p_1 \otimes p_2 \in \mathbb{R}^{2^m}$ is a convolution of $p_1 \in \mathbb{R}^{2^m}$ and $p_2 \in \mathbb{R}^{2^m}$. To be precise,

$$(p_1 \otimes p_2)(x) = \sum_{\substack{y,z\in\mathrm{GF}(2^m)\\ x=y+z}} p_1(y)p_2(z) \text{ for } x \in \mathrm{GF}(2^m).$$

The convolution seems the most complex part of the decoding algorithm. Indeed, the convolutions are efficiently calculated via FFT and IFFT [22], [17]. Increment the iteration round as $\ell{:=}\ell + 1$.

Variable to Check: Each variable node $v = 1, \ldots, N$ in C_1 has two adjacent check nodes since the mother code C_1 is (2, 3)-regular. Let c and c' be the two adjacent check nodes of v. The message $p_{vc}^{(\ell)} \in \mathbb{R}^{2^m}$ sent from v to c is given by

$$p_{vc}^{(\ell)}(x) = \xi p_v^{(0)}(x) p_{c'v}^{(\ell)}(x) \text{ for } x \in \mathrm{GF}(2^m),$$

where ξ is the normalization factor so that

$$\sum_{x\in\mathrm{GF}(2^m)} p_{vc}^{(\ell)}(x) = 1.$$

Tentative Decision: For each $v = 1, \ldots, N$, the tentatively estimated vth transmitted symbol is given as

$$\hat{x}_v^{(\ell)} = \operatorname*{argmax}_{x\in\mathrm{GF}(2^m)} p_v^{(0)}(x) p_{cv}^{(\ell)}(x) p_{c'v}^{(\ell)}(x),$$

where c and c' are the two adjacent check nodes of v. If $\underline{\hat{x}}^{(\ell)} := (\hat{x}_1^{(\ell)}, \ldots, \hat{x}_N^{(\ell)})$ forms a codeword of C_1, in other words, $\underline{\hat{x}}^{(\ell)}$ satisfies every parity-check equation

$$\sum_{v\in\partial c} h_{cv}\hat{x}_v^{(\ell)} = 0 \in \mathrm{GF}(2^m)$$

for all $c = 1, \ldots, M$, the decoder outputs $\underline{\hat{x}}^{(\ell)}$ as the estimated codeword. Otherwise repeat the latter 3 decoding steps. If the iteration round ℓ reaches a predetermined number, the decoder outputs `FAIL`.

The decoder is inherently rate-compatible. Indeed, for decoding the different C_T of rate $1/(3T)$ for $T = 1, 2, \ldots$, the decoder only needs the Tanner graph of the mother code C_1.

IV. Erasure Channel Analysis

In the binary case, we can predict the asymptotic decoding performance of LDPC codes transmitted over the general memoryless binary-input output-symmetric channels in the large code length limit by *density evolution* [4]. Density evolution also can be used to analyze nonbinary LDPC codes [23], [24]. However, for large field size, it becomes computationally intensive and tractable only for the BEC.

Rathi and Urbanke developed the density evolution which enables the prediction of the decoding performance of the nonbinary LDPC codes over the BEC in the limit of large code length. For a given code ensemble, density evolution gives the maximum channel erasure probability at which the decoding erasure probability, averaged over all the LDPC codes in the ensemble goes to zero. The maximum channel erasure probability given by the density evolution is referred to as *the threshold*.

It is shown in [17] that for the transmissions over the BEC with nonbinary LDPC codes defined over $\mathrm{GF}(2^m)$, the decoding results depend on the binary representation, i.e., the primitive element. In other words, two isomorphic fields do not, in general, yield the identical decoding results. Rathi and Urbanke also observed that the difference of the threshold is of the order of 10^{-4} for the different fields. The density evolution [17] is developed for the nonbinary LDPC code ensembles with parity-check matrices defined over the general linear group $\mathrm{GL}(\mathrm{GF}(2), m)$. In this section, we will use the density evolution to evaluate the thresholds of nonbinary LDPC codes defined over $\mathrm{GF}(2^m)$. This is a fair approximation, since in [17], it is reported that the threshold for the code ensemble with parity-check matrices defined over $\mathrm{GF}(2^m)$ and $\mathrm{GL}(\mathrm{GF}(2), m)$ have almost the same thresholds within the order of 10^{-4}.

When the transmission takes place over the BEC and all-zero codeword is assumed to be sent, the messages, described by probability vectors $(p(x))_{x\in\mathrm{GF}(2^m)}$ of length 2^m in general, can be reduced to linear subspaces [17] of $\mathrm{GF}(2)^m$. To be precise, for each message in the BP decoding algorithm, a subset of $\mathrm{GF}(2)^m$

$$\{\boldsymbol{x} \in \mathrm{GF}(2)^m \mid p(x) \neq 0\},$$

forms a linear subspace of $\mathrm{GF}(2)^m$, where $\boldsymbol{x}$ is the binary representation of $x \in \mathrm{GF}(2^m)$.

Define $P^{(\ell)} = \left(P_0^{(\ell)}, \ldots, P_m^{(\ell)}\right)$ and $Q^{(\ell)} = \left(Q_0^{(\ell)}, \ldots, Q_m^{(\ell)}\right)$ as the probability vectors of length $m + 1$ such that $P_i^{(\ell)}$ (resp. $Q_i^{(\ell)}$) is the probability that a message sent from variable (resp. check) nodes has dimension i at the ℓth iteration round of the BP decoding algorithm. The density evolution gives us the update equations of $P^{(\ell)}$ and $Q^{(\ell)}$ for $\ell \geq 0$.

Rathi and Urbanke [17] developed the density evolution for the BEC that tracks probability mass functions of the dimension of the linear subspaces. For $\ell \geq 0$, the density evolution tracks the probability vectors $P^{(\ell)}$ and $Q^{(\ell)}$ which are referred to as *densities*. The initial messages in (2) can be seen as the intersection of T subspaces of the messages received as the channel

outputs. The density of the initial messages is given by $P^{(0)}$ as follows:

$$P^{(0)} = \overbrace{E \boxdot \cdots \boxdot E}^{T \text{ times}},$$
$$E := (E_0, \ldots, E_m),$$
$$E_i := \binom{m}{i} \epsilon^i (1-\epsilon)^{m-i},$$

where ϵ is the channel erasure probability of the BEC. The operator $\boxdot$ is defined as follows:

$$[P \boxdot Q]_k = \sum_{i=k}^{m} \sum_{j=k}^{k+m-i} C_{\boxdot}(m,k,i,j) P_i Q_j,$$

$$C_{\boxdot}(m,k,i,j) := 2^{(i-k)(j-k)} \frac{\begin{bmatrix} i \\ k \end{bmatrix} \begin{bmatrix} m-i \\ j-k \end{bmatrix}}{\begin{bmatrix} m \\ j \end{bmatrix}},$$

where $\begin{bmatrix} m \\ k \end{bmatrix} = \prod_{l=0}^{k-1} \frac{2^m - 2^l}{2^k - 2^l}$ is a 2-Gaussian binomial.

Since the mother code is (2,3)-regular, the update equations of density evolution is given by

$$Q^{(\ell+1)} = P^{(\ell)} \boxtimes P^{(\ell)},$$
$$P^{(\ell+1)} = P^{(0)} \boxdot Q^{(\ell+1)},$$

where the operator $\boxtimes$ is defined as follows:

$$[P \boxtimes Q]_k = \sum_{i=0}^{k} \sum_{j=k-i}^{k} C_{\boxtimes}(m,k,i,j) P_i Q_j,$$

$$C_{\boxtimes}(m,k,i,j) := 2^{(k-i)(k-j)} \frac{\begin{bmatrix} m-i \\ m-k \end{bmatrix} \begin{bmatrix} i \\ k-j \end{bmatrix}}{\begin{bmatrix} m \\ m-j \end{bmatrix}}.$$

Since the messages of dimension 0 corresponds to the successful decoding, the threshold is defined as follows.

$$\epsilon^* := \sup_{\epsilon \in [0,1]} \left\{ \epsilon \in [0,1] \mid \lim_{\ell \to \infty} P_0^{(\ell)} = 1 \right\}.$$

In the large code length limit, if $\epsilon < \epsilon^*$ the reliable transmissions are possible with the proposed C_T.

Fig. 5 draws the thresholds of C_T defined with parity-check matrices over $\mathrm{GL}_m(\mathrm{GF}(2))$ for repetition parameter $T = 1, \ldots, 5$ and $m = 1, \ldots, 10$. The threshold $\epsilon^* = 1/\sqrt[T]{2}$ for the binary case $m = 1$ is decided by the stability condition [19]. It can be seen that the thresholds are not monotonic with respect to m. For repetition parameter $T = 1$, i.e., the mother code has the maximal threshold at $m = 6$. For $T > 2$, the maximal threshold is attained around at $m = 8$.

Fig. 6 compares the proposed codes and the best existing low-rate LDPC codes respect to the thresholds for the BEC. It can be seen that the proposed codes have better thresholds especially for lower rates.

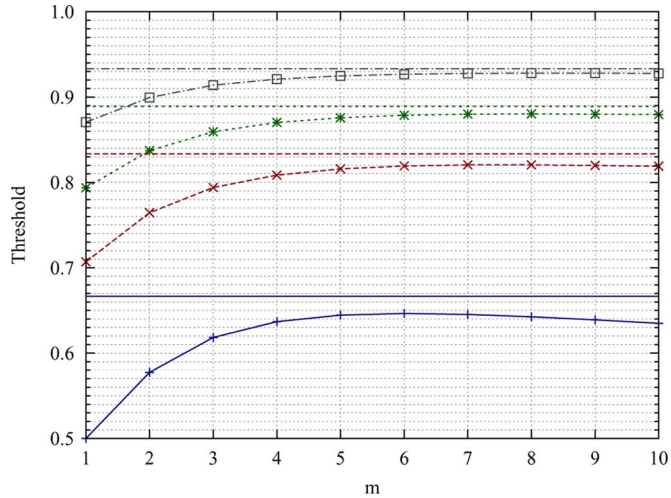

Fig. 5. Thresholds ϵ^* of C_T over GF(2^m) for the BEC and $T = 1, 2, 3$ and 5 from below. The rate is $1/(3T)$. The straight lines show the Shannon limits $1 - 1/(3T)$.

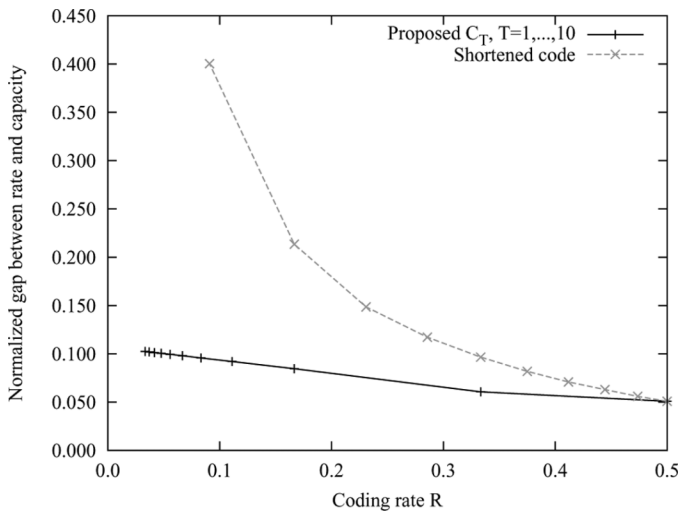

Fig. 6. The asymptotic decoding performance over the BEC of the proposed codes and the best known low-rate codes. One curve corresponds to the proposed code C_T over GF(2^6) of coding rates $R = 1/(3T)$ with repetition parameter $T = 1, \ldots, 10$. The punctured C_1 of rate 1/2 is also plotted. The other curve corresponds to the bit-wise shortened nonbinary LDPC code over GF(2^6) proposed by Klinc [25, Fig. 1]. The vertical axis indicates $(1-\epsilon^*-R)/R$ which is the normalized gap between the capacity $1 - \epsilon^*$ and the rate R, where ϵ^* is the threshold.

V. Numerical Results

In this section, we give some numerical results of the proposed codes. Fig. 7 shows the decoding performance of the proposed code C_2 whose mother code is a (2,4)-regular nonbinary LDPC code defined over GF(2^8). The transmission takes place over the BEC. The compared accumulated LDPC (ALDPC) codes are designed to achieve the capacity in the limit of large code length. It can be seen that the proposed codes exhibit better decoding performance than the ALDPC codes with code length up to 8192. The error floors of the proposed codes can not be observed down to frame error rate 10^{-5} while the ALDPC codes have high error floors even with code length as long as 65 536 bits.

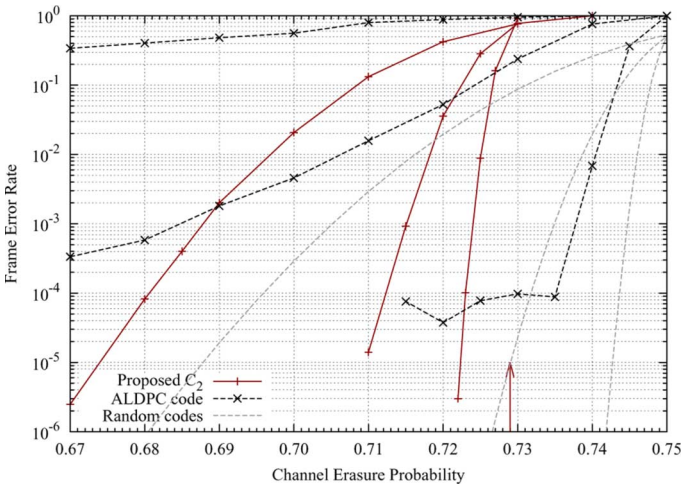

Fig. 7. The solid curve shows the decoding performance of the proposed code C_2 whose mother code is a (2,4)-regular nonbinary LDPC code defined over GF(2^8). The coding rate is 1/4. The transmission takes place over the BEC. The arrow indicates the threshold 0.72898 of C_2. The code length is of length 1024, 8192, and 65 536. For comparison, the decoding performance of accumulated LDPC (ALDPC) codes [26, Fig. 15] is shown. It is known that the ALDPC codes achieve the capacity of the BEC in the limit of large code length and exhibit good decoding performance with finite code length. The frame error rate of corresponding random codes of rate 1/4 under maximum-likelihood decoding are calculated by [27, Eq. (3.2)]. It can be seen that the proposed codes exhibit better decoding performance than the ALDPC codes with code length up to 8192. The error floors of the proposed codes can not be observed down to FER 10^{-5} while the ALDPC codes have high error floors even with code length as long as 65 536 bits.

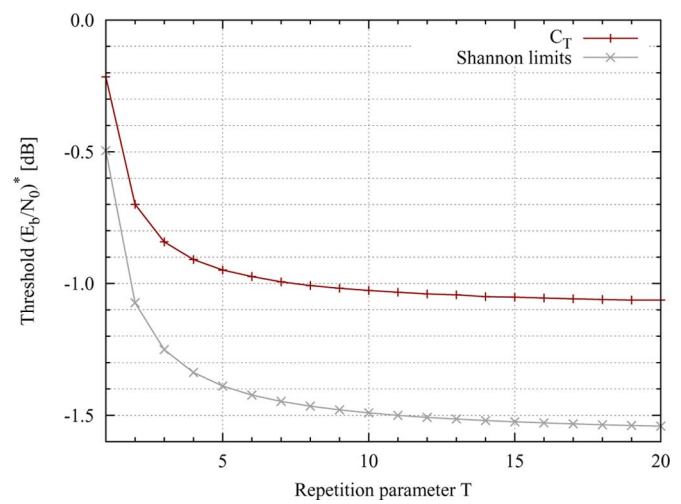

Fig. 8. The thresholds for the AWGN channels of the proposed codes C_T of rate $1/(3T)$ for $T = 1, \ldots, 20$. The codes are defined over GF(2^8).

Fig. 8 shows the thresholds of the proposed codes C_T of rate $1/(3T)$ for $T = 1, \ldots, 20$. The codes are defined over GF(2^8). The threshold values are calculated by the Monte Carlo simulation method. The method was originally suggested in [31, p.22] and an efficient calculation was developed in [32, Sec. VII]. It can be observed that the proposed codes leave a gap to the ultimate Shannon limit $\mathrm{E_b/N_0} = \log_{10}(\ln(2)) \approx -1.59$ [dB] [8] even in the limit of large repetition parameter T. Fig. 9 depicts the simulation results for the AWGN channels of C_2 and C_7 of very long code length. We observe the convergence to a sharp

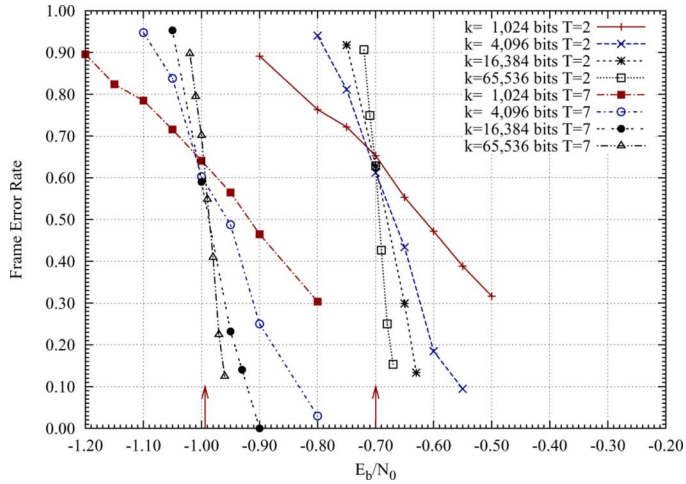

Fig. 9. Frame error rate versus parameter for the proposed codes C_2 and C_7 over GF(2^8) transmitting over the AWGN channel. The rates of C_2 and C_7 are 1/6 and 1/21, respectively. The information length are set to 1024, 4096, 16 834, and 65 536. The arrows indicate the corresponding threshold values. Observe how the curves move closer to these threshold values for increasing codeword lengths.

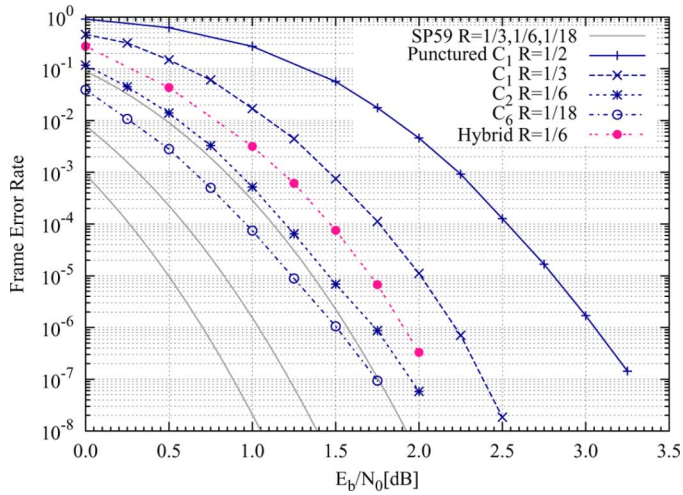

Fig. 10. The frame error rate of the proposed codes C_T for $T = 1, 2, 6$ and hybrid nonbinary LDPC codes. It also shows the performance of rate half punctured mother code C_1. All these codes have 192 information bits. The curves labeled SP59 are the corresponding Shannon's 1959 sphere-packing bound [28]–[30] for rate 1/3, 1/6 and 1/18.

threshold effect at the predicted threshold values as the information length k increases.

We demonstrate the decoding performance of the short and moderate-length proposed codes C_T for $T = 1, 2, 3, 4, 6$ over the binary-input AWGN channels. The mother code C_1 is constructed by the optimization method in [15]. The coefficients $r_{N+1}, \ldots, r_{TN}$ are chosen uniformly at random from $\mathrm{GF}(2^m) \setminus \{0, 1\}$, where $1 \in \mathrm{GF}(2^m)$ is the multiplicative identity. We fix $m = 8$ for its good performance and the computer-friendly representation of byte.

Fig. 10 shows the decoding performance of C_T for $T = 1, 2, 3, 6$ of rates $1/(3T)$. It also shows a hybrid nonbinary LDPC code [16] of rate 1/6 and punctured C_1 of rate 1/2. All these codes have 192 information bits. The proposed code C_2 outperforms the hybrid nonbinary LDPC code which is the best code

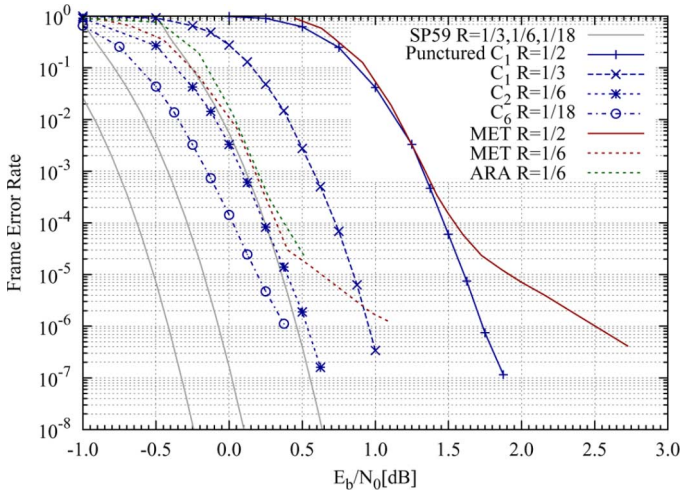

Fig. 11. The frame error rate of the proposed codes C_T for $T = 1, 2, 6$, multiedge type (MET) LDPC code of rate 1/2 [5] and 1/6, and accumulate repeat accumulate (ARA) code [6] of rate 1/6. All these codes have 1024 information bits except that the MET LDPC code of rate 1/2 has 1280 information bits. It also shows the performance of rate half punctured mother code C_1. The curves labeled SP59 are the corresponding Shannon's 1959 sphere-packing bounds for rate 1/3, 1/6 and 1/18.

so far for that rate and code length. The code C_3 of rate 1/9 has about 0.5 [dB] coding gain from C_2 of rate 1/6. As we show on these curves, the proposed construction, although simple, allows to design codes with very low rates without large loss of gap to the Shannon limits.

The same property can be seen for the proposed codes with larger information bits. Fig. 11 shows the decoding performance of C_T for $T = 1, 2, 3, 6$, the binary multiedge type LDPC code of rate 1/2 and 1/6, and the binary ARA code [6] of rate 1/6. All these codes have 1024 information bits except that the MET LDPC code of rate 1/2 has 1280 information bits. It also shows the performance of a punctured mother code C_1 of rate 1/2. Among the codes of rate 1/6, the proposed code C_2 has the best performance both at water-fall and error-floor regions.

As posed in Problem 3, conventional low-rate codes required large code length to exploit the potential performance. It can be seen that the proposed codes exhibit better decoding performance both at small and moderate code length.

VI. Conclusions

We propose nonbinary LDPC codes concatenated with inner multiplicative repetition codes. The performance of the proposed codes exceeds the hybrid nonbinary codes, multiedge type LDPC codes, and ARA codes both at the waterfall and error-floor regions. The encoder and decoder are inherently rate-compatible, and especially the decoder complexity is almost the same as the mother code.

Acknowledgment

The authors would like to thank T. Richardson for providing the data of the multiedge type LDPC code of rate 1/6 in Fig. 11. The authors would also like to thank anonymous reviewers of ISIT2010 and IEEE Transactions on Information Theory, and the associate editor I. Sason for their suggestions and comments. K. K. wishes to thank T. Uyematsu for valuable comments.

References

[1] K. Kasai, D. Declercq, C. Poulliat, and K. Sakaniwa, "Rate-compatible non-binary LDPC codes concatenated with multiplicative repetition codes," in *Proc. 2010 IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2010, pp. 844–848.

[2] R. G. Gallager, *Low Density Parity Check Codes*, ser. Research Monograph Series. Cambridge, MA: MIT Press, 1963.

[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] T. Richardson and R. Urbanke, "Multi-edge type LDPC codes," 2003 [Online]. Available: http://ece.iisc.ernet.in/~vijay/multiedge.pdf

[6] D. Divsalar, S. Dolinar, and C. Jones, "Low-rate LDPC codes with simple protograph structure," in *Proc. 2005 IEEE Int. Symp. Inf. Theory (ISIT)*, Sep. 2005, pp. 1622–1626.

[7] G. Yue, L. Ping, and X. Wang, "Generalized low-density parity-check codes based on Hadamard constraints," *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 1058–1079, Mar. 2007.

[8] S. Haykin, *Communication Systems*, 4th ed. New York: Wiley, 2001.

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

[10] W. Chang and J. Cruz, "Nonbinary LDPC codes for 4-kB sectors," *IEEE Trans. Magn.*, vol. 44, no. 11, pp. 3781–3784, Nov. 2008.

[11] I. Djordjevic and B. Vasic, "Nonbinary LDPC codes for optical communication systems," *IEEE Photon. Technol. Lett.*, vol. 17, no. 10, pp. 2224–2226, Oct. 2005.

[12] 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, Jun. 2009.

[13] M. Arabaci, I. Djordjevic, R. Saunders, and R. Marcoccia, "High-rate nonbinary regular quasi-cyclic LDPC codes for optical communications," *J. Lightw. Technol.*, vol. 27, no. 23, pp. 5261–5267, Dec. 2009.

[14] 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.

[15] C. Poulliat, M. Fossorier, and D. Declercq, "Design of regular $(2d, c)$-LDPC codes over GF(q) using their binary images," *IEEE Trans. Commun.*, vol. 56, no. 10, pp. 1626–1635, Oct. 2008.

[16] L. Sassatelli, D. Declercq, and C. Poulliat, "Low-rate non-binary hybrid LDPC codes," in *Proc. 5th Int. Symp. Turbo Codes Related Topics*, Sep. 2008, pp. 225–230.

[17] 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.

[18] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: Elsevier, 1977.

[19] T. Richardson and R. Urbanke, *Modern Coding Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2008.

[20] J. Justesen, "Class of constructive asymptotically good algebraic codes," *IEEE Trans. Inf. Theory*, vol. IT-18, no. 5, pp. 652–656, Sep. 1972.

[21] M. Davey and D. MacKay, "Low density parity check codes over GF(q)," in *Proc. Inf. Theory Workshop*, Jun. 1998, pp. 70–71.

[22] D. Declercq and M. Fossorier, "Decoding algorithms for nonbinary LDPC codes over GF(q)," *IEEE Trans. Commun.*, vol. 55, no. 4, pp. 633–643, Apr. 2007.

[23] A. Bennatan and D. Burshtein, "On the application of LDPC codes to arbitrary discrete-memoryless channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 3, pp. 417–438, Mar. 2004.

[24] G. Li, I. Fair, and W. Krzymien, "Density evolution for nonbinary LDPC codes under Gaussian approximation," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 997–1015, Mar. 2009.

[25] D. Klinc, J. Ha, and S. McLaughlin, "Optimized puncturing and shortening distributions for nonbinary LDPC codes over the binary erasure channel," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, Sep. 2008, pp. 1053–1058.

[26] H. Pfister and I. Sason, "Accumulate repeat accumulate codes: Capacity-achieving ensembles of systematic codes for the erasure channel with bounded complexity," *IEEE Trans. Inf. Theory*, vol. 53, no. 6, pp. 2088–2115, Jun. 2007.
[27] C. Di, D. Proietti, I. Telatar, T. Richardson, and R. Urbanke, "Finite-length analysis of low-density parity-check codes on the binary erasure channel," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1570–1579, Jun. 2002.
[28] C. E. Shannon, "Capacity of the band-limited Gaussian channel," *Bell System Tech. J.*, vol. 38, pp. 611–656, May 1959.
[29] A. Valembois and M. Fossorier, "Sphere-packing bounds revisited for moderate block lengths," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 2998–3014, Dec. 2004.
[30] G. Wiechman and I. Sason, "An improved sphere-packing bound for finite-length codes over symmetric memoryless channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 5, pp. 1962–1990, May 2008.
[31] M. Davey, "Error-correction using low-density parity-check codes," Ph.D. dissertation, Univ. Cambridge, Cambridge, U.K., 1999.
[32] L. Sassatelli and D. Declercq, "Nonbinary hybrid LDPC codes," *IEEE Trans. Inf. Theory*, vol. 56, no. 10, pp. 5314–5334, Oct. 2010.

Kenta Kasai (M'10) received the B.E., M.E., and Ph.D. degrees from the Tokyo Institute of Technology, Tokyo Japan, in 2001, 2003 and 2006, respectively.

Since 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. From 2008 to 2009, he was a visiting researcher at ETIS laboratory, Ecole Nationale Supérieure de l'Electronique et de ses Applications, Cergy-Pontoise, France. His current interests include coding theory.

David Declercq (M'07) was born in June 1971. He graduated his Ph.D. in Statistical Signal Processing in 1998. He worked on a new Gaussianity test based on Hermite polynomials properties, and the characterization and the blind identification of nonlinear time series. After his Ph.D., he oriented his research towards digital communications, and especially coding theory and iterative decoder design. He started to work on LDPC codes in 1999, both from the code and decoder design aspects.

Since 2003, he focused on studying and developing LDPC codes and decoders in high order Galois fields GF(q), with $q \gg 2$. A large part of his research projects are related to nonbinary LDPC codes. He mainly investigated two directions: i) the design of GF(q) LDPC codes for short and moderate lengths, and ii) the simplification of the iterative decoders for GF(q) LDPC codes with complexity/performance tradeoff constraints.

David Declercq published more than 20 papers in major journals (IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE TRANSACTIONS ON INFORMATION THEORY, *Communication Letters*, EURASIP JWCN), and more than 70 papers in major conferences in ICT. He is currently full professor at the ENSEA in Cergy-Pontoise, France, a graduate school in Electrical Engineering. He is a member of the ETIS laboratory, general secretary of the National GRETSI association, and member of the GdR-ISIS direction team. He is currently the recipient of junior position at the "Institut Universitaire de France."

Charly Poulliat (M'09) received the E.E. degree from the Ecole Nationale Supérieure de l'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 postdoctoral researcher at UH coding group supervised by Pr. Marc Fossorier, University of Hawaii at Manoa, HI, USA. In December 2010, he received his Accreditation to Supervise Research (Habilitation à Diriger des Recherches) from the University of Cergy-Pontoise, France. He is currently an associate 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, signal processing for digital communications.

Kohichi Sakaniwa (M'88–SM'04) received the 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 Communications and Integrated Systems, Graduate School of Science and Engineering, both in the Tokyo Institute of Technology. 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, IEICE Japan, Information Processing Society of Japan, and Institute of Image Information and Television Engineers of Japan.