Iterative Decoding Based on Concatenated Belief Propagation for CRC-Aided Polar Codes

Satoshi Tajima*, Takumi Takahashi*, Shinsuke Ibi*, and Seiichi Sampei* * Graduate School of Engineering, Osaka University, Suita, Japan

E-mail: {tajima@wcs., takahashi@wcs., ibi@, sampei@}comm.eng.osaka-u.ac.jp

Abstract—This paper proposes a novel iterative decoder based on concatenated belief propagation (BP) for CRC-aided polar codes. Compared to the conventional BP-based decoders for polar codes, soft cancellation (SCAN) decoder can generate a log likelihood ratio (LLR) of coded bit with lower computational complexity without sacrificing the detection capability. Unfortunately, its performance is not as good as that of CRC-aided successive cancellation list decoder (SCLD) although SCAN decoder has advantage of hardware implementation. To compensate the performance gap, we exploit CRC structure for not only error detection but also error correction with the assistance of its error correction capability at a short code length by exchanging LLRs between SCAN decoder and BP decoder on the basis of CRC. Moreover, the sub-optimal criterion for selecting a parity check matrix of CRC for BP decoder is proposed. Finally, computer simulations are conducted to confirm the validity of our proposed method. The proposed method can obtain the gain of about 0.6 dB at BER = 10^{-3} compared to the native SCAN decoder without requiring huge memory size as in SCLD.

I. INTRODUCTION

In 2009, Arikan proposed a polar code based on channel polarization phenomena [1], which is universally recognized as a major breakthrough in coding theory. The most noteworthy point of polar codes is achievability of the Shannon limit for symmetric binary-input memoryless channels by using simple successive cancellation decoder (SCD) with low encoding and decoding complexity. Moreover, in 2016, the third generation partnership project (3GPP) agreed to adopt polar codes for the enhanced mobile broadband (eMBB) control channels for the 5G new radio (NR). As a result, polar codes are gaining attention more and more.

The native SCD is capable of achieving high decoding capability when the code length is sufficiently long. However, if the code length is short, the channel polarization effect cannot be adequately experienced, resulting in poor decoding performance. To remedy the drawback, which is induced by the poor channel polarization, several decoding algorithms have been proposed so far. The sophisticated algorithms are roughly classified into two types: successive cancellation list decoding (SCLD) and belief propagation (BP) decoding.

Successive canceller suffers from error propagation issues. The SCLD applies list decoding that select W higher likelihood candidates as survival paths. The list structure can mitigate the negative impacts of the error propagation [2]. However, the decoding capability is worse than low density parity check (LDPC) codes [3]. To cope with the drawback, cyclic redundancy check (CRC) aided list decoding is helpful in finding better survival paths. As a result, in short code length, its performance is better than the LDPC at the expense of computational complexity. Furthermore, we should pay attention that the SCLD is not suitable for generating loglikelihood ratios (LLR) of a coded bit, which is exploited for performing statistical signal processing in bit interleave coded modulation (BICM)-iterative detection (ID) as well as turbo equalizer [4].

For generating reasonable LLR, Arikan's BP decoding method has been proposed in [5]. BP decoder iteratively performs message passing on the factor graph (FG) of the polar code to improve the detection capability gradually. Unfortunately, the computational complexity of Arikan's BP decoder is higher than SCLD. For reducing the computational complexity to find LLR of a coded bit, soft cancellation (SCAN) decoder has been proposed [6], [7]. However, its performance is not as good as CRC-aided SCLD.

To compensate the performance gap, this paper exploits CRC structure even in SCAN decoder. In this case, CRC is utilized for not only error detection but also error correction with the assistance of its error correction capability at a short code length. In the conventional SCAN decoding method, iterative decoding is performed only on the FG of polar codes. In addition, BP decoder for the CRC structure is serially concatenated with SCAN decoder for polar codes in the present paper. For the serially concatenated code, iterative LLR exchange between SCAN and BP decoders is effective in obtaining enhanced LLR.

A problem in performing BP decoding based on the CRC structure is a presence of short cycle (SC) depicted in a Tanner graph (TG) of parity check matrix. If TG contains many SCs, strict probabilistic marginalization cannot be performed at the sum-product algorithm (SPA) variable node, and there is a disadvantage that its decoding performance is severely degraded. In order to solve this inconvenience, we propose optimal selection criteria for parity check matrix in this paper.

The paper is organized as follows. In Sect. II, a signal model is defined. The polar coded transmission system and the algorithm of SCAN decoder are explained in Sect. III. In Sect. IV, we propose an iterative decoding algorithm for concatenated structure between BP decoder based on CRC and SCAN decoder. Then, we discuss a problematic SC when operating SPA based on CRC, and propose selection criteria for parity check matrix. In Sect. V, the proposed method is validated by computer simulations. Finally, Sect. VI concludes



Fig. 1: A schematic of polar coded transceiver.

this paper.

II. SIGNAL MODEL

Let us consider polar codes of code length N bits and information bit length K bits with coding rate K/N. The polar coded transmission model is shown in Fig. 1. At the transmitter, information bits $d = [d_0, \ldots, d_k, \ldots, d_{K-1}]$ is encoded by channel encoder C, resulting in coded bits x = $[x_0, \ldots, x_n, \ldots, x_{N-1}]$. The resultant coded bits are modulated by binary shift keying (BPSK) \mathcal{M} to yield transmitted symbols $s = [s_0, \ldots, s_n, \ldots, s_{N-1}] \in S = \{\sqrt{E_s}, -\sqrt{E_s}\}^N$, i.e. $s_n = -2x_n + 1$. where E_s denotes the average energy of transmitted symbols. Assuming additive white Gaussian noise (AWGN) channels, the receiver observes received symbols $y = [y_0, \ldots, y_n, \ldots, y_{N-1}]$, which is represented as

$$\boldsymbol{y} = \boldsymbol{s} + \boldsymbol{z},\tag{1}$$

where $\boldsymbol{z} = [z_0, \ldots, z_n, \ldots, z_{N-1}]$ denotes a complex-valued AWGN vector, whose elements obey zero mean and variance of one-sided noise power spectrum density N_0 . The received symbols \boldsymbol{y} is softly demodulated by symbol demapper \mathcal{M}^{-1} for computing LLR of a coded bit, which is given by

$$r_n = \ln \frac{p(y_n | x_n = 0)}{p(y_n | x_n = 1)},$$
(2)

where $p(y_n|x_n)$ is probability density function of the observation y_n . Substituting (1) into (2), the LLR is simplified as

$$r_n = \frac{4\sqrt{E_s}}{N_0} \Re\left\{y_n\right\},\tag{3}$$

where $\Re\{\cdot\}$ indicates the real part of complex values. On the basis of the resultant LLR, channel decoder C^{-1} detects estimates of information bits $\hat{d} = [\hat{d}_0, \dots, \hat{d}_k, \dots, \hat{d}_{K-1}]$.

III. POLAR ENCODER AND SCAN DECODER

A. Construction of polar codes

In the encoder C, an information bit vector d is mapped to a vector $u = [u_0, u_1, \ldots, u_{N-1}]$ on the position corresponding to an index set \mathcal{I} $(|\mathcal{I}| = K)$. On the other hand, denoting complementary set of \mathcal{I} as \mathcal{I}^c $(|\mathcal{I}^c| = N - K)$, 0 is mapped to the vector u on the position corresponding to the complementary index set \mathcal{I}^c . The N-K zero elements on the \mathcal{I}^c are referred to as frozen bits, and the index set is known to both the encoder and the decoder. The position of frozen bits are typically determined at channels with lower mutual information [8] ¹. Then, coded bits x are obtained by

$$\boldsymbol{x} = \boldsymbol{u}\boldsymbol{B}_N\boldsymbol{F}_N,\tag{4}$$



Fig. 2: An example of FG of polar codes (N = 8).



Fig. 3: Unit graph for polar codes.

where matrices B_N and F_N are a bit-reversal and a generator matrix of polar codes, respectively. The matrix F_N is defined by

$$\boldsymbol{F}_N = \boldsymbol{F}_2^{\otimes m},\tag{5}$$

where $m = \log_2 N$, $(.)^{\otimes m}$ denotes the *m*-th Kronecker power, and

$$\boldsymbol{F}_2 = \left(\begin{array}{cc} 1 & 0\\ 1 & 1 \end{array}\right). \tag{6}$$

B. Soft Cancellation Decoder

SCAN decoder performs over the FG of polar codes. An example of the FG of a polar code with code length N = 8 is illustrated in Fig. 2. There are N(m+1) nodes in the FG when length $N = 2^m$. These nodes are classified into m + 1 classes indexed by λ , and each class consists of 2^{λ} groups indexed by φ . Furthermore, each group contains $2^{m-\lambda}$ nodes indexed by ω . An arbitrary node can be denoted by these parameters $(\lambda, \varphi, \omega)$ uniquely.

Each node has two memories of LLRs L and R. LLR belief $L_{\lambda}(\varphi, \omega)$ at the $(\lambda, \varphi, \omega)$ node propagates from left to right on the FG. By contrast, $R_{\lambda}(\varphi, \omega)$ does from right to left. Note that $L_{\lambda}(\varphi, \omega)$ of the most left side $L_0(0, \omega)$ is the received channel LLR r_{ω} and initial values of $R_m(\varphi, 0)$ on the most right side has constant LLRs, where $R_m(\varphi, 0) = 0$ if u_{φ} is an information bit and $R_m(\varphi, 0) = +\infty$ if it is a frozen bit. The FG in Fig. 2 is constructed by serial and parallel concatenation

¹In this paper, for simplicity, *K* channels with large channel capacity of *m*-times polarized binary erasure channel (BEC) are selected for transmitting information bits.

Fig. 4: A schematic of CRC-aided polar-coded transceiver.

of unit graphs shown in Fig. 3. The message passing rules on the unit graph are summarized as follows:

$$L_{\lambda+1}(\varphi_2, \omega_2) = f(R_{\lambda+1}(\varphi_3, \omega_3) + L_{\lambda}(\varphi_1, \omega_1), L_{\lambda}(\varphi_0, \omega_0)), \quad (7)$$
$$L_{\lambda+1}(\varphi_3, \omega_3)$$

$$= f(R_{\lambda+1}(\varphi_2,\omega_2), L_{\lambda}(\varphi_0,\omega_0)) + L_{\lambda}(\varphi_1,\omega_1), \quad (8)$$

$$R_{\lambda}(\varphi_0,\omega_0)$$

$$= f(R_{\lambda+1}(\varphi_2, \omega_2), R_{\lambda+1}(\varphi_3, \omega_3) + L_{\lambda}(\varphi_1, \omega_1)),$$
(9)
$$R_{\lambda}(\varphi_1, \omega_1)$$

$$= f(R_{\lambda+1}(\varphi_2,\omega_2),L_{\lambda}(\varphi_0,\omega_0)) + R_{\lambda+1}(\varphi_3,\omega_3),(10)$$

where the function f(a, b) is defined as

$$f(a,b) \triangleq 2 \tanh^{-1} \left[\tanh\left(\frac{a}{2}\right) \times \tanh\left(\frac{b}{2}\right) \right].$$
 (11)

IV. CRC-AIDED SCAN ITERATIVE DECODER

A. CRC Error Correction

The CRC encoder appends parity bits of length J bits $p = [p_0, \ldots, p_{J-1}]$ to the end of information block d. As a result, we have CRC-coded bits of length K + J bits $b = [d, p] = [b_0, \ldots, b_{K+J-1}]$. While CRC codes are usually used for an error detection only, they might have error correction capability, thanks to the redundancy of parity bits. When information bit length K is large, the coding rate K/(K + J) is high, resulting in weak error correction capability. However, when information bit length K is enough short, the error correction capability is significant. The CRC-coded block b could be regarded as a binary liner block code, and the SPA decoder is a useful decoding algorithm for such block codes.

B. Iterative Decoding between SCAN and CRC Decoders

The CRC-aided polar code implicitly has a structure of serial concatenated code in which polar and CRC codes are inner and outer codes, respectively. For the concatenated structure, iterative decoding based on Turbo principle is effective in improving the reliability of LLRs [9]. A configuration of the CRC-aided polar-coded transceiver is depicted in Fig. 4. At the transmitter, as mentioned before, parity bits p are added to the end of information bits d by CRC encoder. Then, coded bits x is obtained by the polar encoder explained in Sect. III. The resultant coded bits are modulated by BPSK. LLR $\alpha = [\alpha_0, \dots, \alpha_{K+J-1}]$ is obtained in each iteration, and delivered to SPA decoder of the CRC. CRC decoder performs error corrections by SPA to yield LLR $\beta = [\beta_0, \dots, \beta_{K+J-1}]$. Then, subtracting α from β , the extrinsic LLR which are fed back to polar SCAN decoder is obtained.

This LLR exchange between two decoders is performed until the parity check of the CRC is satisfied or the iteration number reaches an arbitrary maximum count. When the iteration is over, we detect the information bits d from the output LLR of information bit of SPA decoder $\gamma = [\gamma_0, \ldots, \gamma_k \ldots, \gamma_{K-1}]$ as

$$\hat{d}_k = \begin{cases} 0 & (\gamma_k \ge 0) \\ 1 & \text{otherwise} \end{cases}.$$
 (12)

C. SPA Decoding for CRC

Now let us focus on the parity check matrix of CRC. According to the generator polynomial to be used, the $K \times (K + J)$ generator matrix is represented as

$$\boldsymbol{G} = [\boldsymbol{I}_J | \boldsymbol{P}], \tag{13}$$

where I_J is a $J \times J$ identity matrix and P is a generator matrix for generating the parity bits of CRC. On the other hand, the parity check matrix H can be derived as

$$\boldsymbol{H} = \begin{bmatrix} \boldsymbol{P}^{\mathrm{T}} | \boldsymbol{I}_J \end{bmatrix}, \qquad (14)$$

where $.^{T}$ indicates a matrix transpose. The generator matrix G and the parity check matrix H always satisfy a parity check equation, which is represented as

$$\boldsymbol{G}\boldsymbol{H}^{\mathrm{T}} = \boldsymbol{P} + \boldsymbol{P} = \boldsymbol{0}. \tag{15}$$

As long as no SCs are included in the TG of the parity check matrix H, SPA can perform strict probabilistic marginalization and is an optimal soft-input soft-output iterative decoding algorithm based on BP [10]. By inputting LLRs of information bits from the SCAN decoder to the SPA decoder of CRC as prior information, more reliable LLRs of information bits may be obtained. However, when SCs exist in the TG of parity check matrix, it is subject to loopy propagation, and the output beliefs from a certain variable node is propagated back to the same node after several iterations [11]. As a result, belief propagation among the nodes has strong correlations, resulting in the significant degradation of decoding performance in SPA. Unfortunately, the negative impacts of correlations becomes more severe as the length of the loops becomes shorter. It is well known that the performance deterioration is noticeable, especially when the length of SC is 4. In other words, we may improve the performance of SPA decoder by using a parity check matrix with a small number of SCs of length 4.

When the generator matrix G is not a square matrix, there are a lot of parity check matrices H satisfying the parity check equation of (15). Therefore, there is a possibility to find an appropriate parity check matrix H with a few SCs of length



Fig. 5: Shape of parity check matrices (K = 40).

4. The number of SCs of length 4 in the TG of check matrix *H* can be calculated by [12],

$$\eta(\boldsymbol{H}) = \sum_{i=1}^{K} \sum_{j=i+1}^{K} \begin{pmatrix} \left[\boldsymbol{H} \boldsymbol{H}^{\mathrm{T}} \right]_{i,j} \\ 2 \end{pmatrix}, \qquad (16)$$

where $[\mathbf{A}]_{i,j}$ denotes the *i*-th row and *j*-th column (i,j) element of matrix \mathbf{A} and $\begin{pmatrix} a \\ b \end{pmatrix} = {}_{a}\mathbf{C}_{b}$ is the number of combinations.

For the simplicity, we consider shifts of the identity matrix I_J to an arbitrary θ -th starting column ($\theta = 1, \ldots, K + 1$) by applying basic row operations on matrices to find the appropriate check matrix. The resultant matrix is denoted by H_{θ} . Then, the parity check matrix with the smallest number of contained SCs of length 4 is given by

$$\hat{\theta} = \arg \min \eta(\boldsymbol{H}_{\theta}). \tag{17}$$

Fig. 5 shows the parity check matrices H_1 and H_{34} in the case of K = 40, respectively. The check matrix H_{34} in (b) includes the least number of SCs of length 4 in TG, which is obtained by (17). The number of SCs of length 4 included in H_{34} is 3,407, whereas it is 9,925 in H_1 .

V. SIMULATION RESULTS

We have conducted several computer simulations to confirm the validity of the proposed decoding method. Tab. I shows the simulation conditions. As a CRC, CRC-24 (J = 24) is used. The generator polynomial of CRC-24 is given by

$$g(x) = x^{24} + x^{10} + x^9 + x^6 + x^4 + x^3 + x + 1.$$
 (18)

The length of information bits K is 40. The length of the polar code is N = 128 with half coding rate. K channels with large channel capacity of m-times polarized BEC are selected for the index set of information bits \mathcal{I} . The erasure rate ε of BEC is decided by performing computer simulation assuming SCD

TABLE I: Simulation conditions.

Information bit length	K = 40
Outer channel encoder	CRC-24
Inner channel encoder	half-rate polar code
polar encoded bit length	N = 128
Num. of iterations for SPA	32
Num. of iterations for SCAN	8
Modulator	BPSK
Channel model	AWGN



Fig. 6: BLER performance of several types of decoders.

and selecting the one with the best performance. The modulation scheme is BPSK, and the channel model is AWGN. The maximum number of local iterations inside SPA and global iterations of SCAN are 32 and 8, respectively.

Fig. 6 shows the BLER performances of CRC-aided polar codes with several types of decoders. In "CRC + SCAN (i)", CRC is used only for error detection. On the other hand, "CRC + SCAN (ii)" is the proposed iterative decoding scheme with the aid of the error correction capability of CRC based on H_1 . "CRC + SCAN (iii)" is proposed method based on H_{34} with the minimum numbers of SCs with length 4. As a comparison with leading-edge method, the performance of SCLD with list size W = 32 is presented. Compared to "CRC + SCAN (i)", the proposed method "CRC + SCAN (ii) improves the performance of SCAN decoder, but the improvement is slight and not sufficient due to the large number of SCs included in H_1 . By contrast, "CRC + SCAN (iii)" can significantly improve the performance with the assistance of the appropriate check matrix H_{34} . More specifically, the proposed method can obtain the gain of about 0.6 dB at BLER = 10^{-3} compared to the native SCAN decoding "CRC + SCAN (i)". Unfortunately, there is still a gap of about 1.2 dB compared to the SCLD. However, required memory size is smaller than SCLD as

Decoding method	Total memory for decoding
SCD	3(2N-1)
SCLD	W(6N+3m+2)
SCAN	2N(m+1)
Proposed Method	2N(m+1) + 2J(K+J)

TABLE II: Memory size required for different decoders of polar codes.

discussed following.

Let us shift our focus to the number of memories required to decode polar codes, where one memory is required to store one LLR value. Here, we define L and R to denote the memories required to store the LLRs passed from left to right and from right to left in the Tanner graph of polar codes. When the length of polar code is N, the SCD requires 2N-1memories for L and 2(2N-1) memories for R. As a result, 3(2N-1) memories are required [2], [13]. On the other hand, in SCLD, the number of memories required for L and R are W(2N-1) and 2W(2N-1), where W is the decoding list size [2], and another 3W(m+1) + 2W memories are needed for path mapping. Thus, the total number of memories required for SCLD is W(6N+3m+2). By contrast, in SCAN decoding, 2N(m+1) memories are required because N(m+1)nodes need to keep the values of L and R, respectively [6] In addition, 2J(K + J) memories for store LLRs are required in the SPA decoding on the basis of CRC included in the proposed method. Therefore, the total number of memories for proposed decoding is 2N(m+1) + 2J(K+J). Tab. I summarizes the total number of memories required to decode polar codes with different decoding methods.

Fig. 7 shows the number of required memories of each decoding method according to the code length N, where the CRC length is J = 24, the code rate of polar codes is 1/2. The list size of SCLD is W = 32. Obviously, the number of memories of our proposed method is far less than that of SCLD, which is advantageous in hardware implementation. Under the condition N = 128, K = 40, the number of memories required for the proposed method is 5,120 while the SCLD with CRC requires 25,312. Remarkably, the number of memories required for proposed method is about 1/5 of that of SCLD.

VI. CONCLUSIONS

In this paper, we proposed a novel iterative decoder design based on concatenated belief propagation for CRC-aided polar codes by exploiting CRC structure. CRC was utilized for not only error detection but also error correction with the assistance of the error correction capability of the CRC at a short code length. Furthermore, to solve the performance degradation of SPA-based decoding induced by the SCs included in the parity check matrix of the CRC, the criterion for selecting the parity check matrix based on the number of SCs of length 4 was applied. Finally, we demonstrated the proposed method can obtain the gain of about 0.6 dB



Fig. 7: Number of memories required for different decoders.

at BER = 10^{-3} compared to the native SCAN decoding by computer simulations. Compared to SCLD, the proposed method can decode polar codes with lower required memory spaces. However, there is still a large performance gap between the BP-based decoder and SCLD. Therefore, as our future work, we are considering the development of our method to improve this deterioration.

ACKNOWLEDGMENT

A part of this work was nancially supported by JSPS KAKENHI Grant Number JP18H03765, Japan.

REFERENCES

- [1] E. Arikan, "Channel polarization: A method for constructing capacityachieving codes for symmetric binary-input memoryless channels," IEEE Trans. Info. Theory, vol.55, no.7, pp.3051-3073, July 2009.
- [2] I. Tal and A. Vardy, "List decoding of polar codes," 2011 IEEE Int. Symp. Inf. Theory Proc., pp.15, IEEE, July 2011. R. G. Gallager, "Low-density parity-check code," Research Monograph
- [3] series, Cambridge, MIT Press, 1963
- C. Douillard, M. Jzquel, C. Berrou, D. Electronique, A. Picart, P. Didier, [4] and A. Glavieux, "Iterative correction of intersymbol interference: Turboequalization," European Transactions on Telecommunications, vol. 6, no. 5, pp. 507-511, 1995.
- [5] E. Arikan, "A performance comparison of polar codes and Reed-Muller codes," Communications Letters, IEEE, vol. 12, no. 6, pp. 447-449, June 2008.
- [6] U. U. Fayyaz and J. R. Barry, "Polar codes for partial response channels," in IEEE Int. Conf. Commun., Budapest, Hungary, June 2013, pp. 4337-
- [7] U. U. Fayyaz and J. R. Barry, "Low-complexity soft-output decoding of polar codes," IEEE Sel. Commun. vol. 32, no. 5, pp. 958966, May 2014.
- [8] H. Vangala, E. Viterbo, and Y. Hong, "A comparative study of polar code constructions for the AWGN channel," Jan. 2015.
- [9] J. Hagenauer, E. Offer, and L. Papke, "Iterative decoding of binary block and convolutional codes," IEEE Trans. on Inf. Theory, vol. 42, pp. 429-445, Mar. 1996.
- [10] V. Kumar, O. Milenkovic, and K. Prakash, "On graphical representations of algebraic codes suitable for iterative decoding," in Proc. 39th Conf. Information Sciences and Systems, Baltimore, MD, Mar. 2005.
- [11] M. Kevin, W. Yair And J. Michael, "Loopy belief propagation for approximate inference: An empirical study," Proceedings of the 15th Conference on Uncertainty in Artificial Intelligence, Jan. 2013.
- [12] S. Sankaranarayanan and B. Vasic, "Analysis of iterative erasuredecoding of linear block codes: a parity-check orthogonalization approach," in Proc. 42nd Annual Allerton Conference on Communication, Control, and Computing, pp.1682-1691, Sept. 2004.
- Y. Wang, K. R. Narayanan, and Y. C. Huang, "Interleaved concatenations [13] of polar codes with BCH and convolutional codes," IEEE Journal on Selected Areas in Communications, vol. 34, no. 2, pp. 267-277, Feb. 2016.