Protograph-Based Design for QC Polar Codes

Toshiaki Koike-Akino and Ye Wang
Mitsubishi Electric Research Laboratories (MERL), 201 Broadway, Cambridge, MA 02139, USA.
Email: {koike, yewang}@merl.com

Abstract—We propose a new family of polar coding which realizes high coding gain, low complexity, and high throughput by introducing a protograph-based design. The proposed technique called as quasi-cyclic (QC) polar codes can be highly parallelized without sacrificing decoding complexity. We analyze short cycles in the protograph polar codes and develop a design method to increase the girth. Our approach can resolve the long-standing unsolved problem that belief propagation (BP) decoding does not work well for polar codes due to the inherently short cycles. We demonstrate that a high lifting factor of QC polar codes can improve the performance and that QC polar codes with BP decoding can outperform conventional polar codes with state-of-the-art list decoding. Moreover, we show that a greedy pruning method can improve the performance-complexity trade-off.

I. INTRODUCTION

Capacity-approaching forward error correction (FEC) based on low-density parity-check (LDPC) codes [1]–[14] have made a great contribution to increasing data rates of wireless and optical communication systems. However, the pursuit of high FEC performance has led to a significant increase in power consumption and circuit size. Hence, attaining a good trade-off between performance and computational complexity is of great importance. In addition, recent high-performance LDPC codes usually require very large codeword lengths, whereas shorter FEC codes are preferred [15] for latency-constrained systems, such as Internet-of-Things (IoT) applications.

Polar codes [16]–[41] have drawn much attention as alternative capacity-approaching codes in place of LDPC codes for short block lengths, in particular for the fifth-generation (5G) networks. Besides encoder design methods [23]–[28], a number of decoder algorithms were developed [29]–[31]. With successive cancellation list (SCL) decoding [19], polar codes can be highly competitive with state-of-the-art LDPC codes. To date, various extended versions based on polar coding have also been proposed in literature; e.g., nonbinary [32], mixed-kernel [33], [34], irregular [35], [36], concatenated [37]–[39], convolutional [40], and turbo product coding [41].

In this paper, we introduce a novel family of protograph-based polar codes, which we call quasi-cyclic (QC) polar codes having circulant permutation at proto-polarization units as illustrated in Fig. 1. With a proper circulant shift value, we show that the QC polar codes can eliminate short cycles in the code graph, which achieves a remarkable breakthrough toward resolving the long-standing issue that the belief-propagation (BP) decoding does not perform well for polar codes. In the QC polar codes, highly parallel short polar codes are coupled to achieve performance comparable to longer polar codes while maintaining the computational complexity as low as that of short polar codes. The contributions of this paper are summarized as follows:

- **Protograph-based polar codes:** We propose a new family of protograph polar codes. To the best of the authors’ knowledge, the concept of protograph codes has never been applied to such non-parity-check codes.
- **QC polar codes:** We introduce highly parallelizable QC polar codes, a special case of protograph, with circulant permutations at the proto-polarization units.
- **Complexity analysis:** We show that the computational complexity of the proposed QC polar codes can be significantly decreased with a protograph lifting factor.
- **Girth analysis:** We analyze short cycles of the protograph polar codes, and develop a design method to increase the girth. Eliminating short cycles enables BP decoding to properly work for the QC polar codes.
- **State-of-the-art performance:** We demonstrate that the QC polar codes with shallow polarization can achieve competitive performance of deep polarization codes.
- **Irregular pruning:** Further complexity reduction and performance improvement are shown with irregular pruning of polarization to cut loops in the protograph.

II. BASICS OF POLAR CODES

A. Polar Encoding

An $n$-stage polar code with $K$ information bits and $N = 2^n$ encoded bits uses an $N \times N$ generator matrix $G^\otimes n$ for

![Fig. 1: Four-stage polarization: QC polar codes $(2^4, 2^8)$ having circulant shift values for 32 proto-polarization units.](image)
encoding, where $[\cdot]^{\otimes n}$ denotes the $n$-fold Kronecker power and $G$ is a binary kernel matrix defined as

$$G = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}. \quad (1)$$

Let $u = [u_1, u_2, \ldots, u_N]^T$ and $x = [x_1, x_2, \ldots, x_N]^T$ respectively denote the column vectors of input bits and encoded bits. The codeword (for non-systematic codes) is given by $x = G^{\otimes n} Bu$, where the matrix multiplications are carried out over the binary field (i.e., modulo-2 arithmetic), and $B$ denotes an $N \times N$ bit-reversal permutation matrix [16]. Due to the nature of the Kronecker product, polar encoding and decoding can be performed at a complexity on the order of $O(N \log_2 N)$. The multi-stage operation of the Kronecker products gives rise to the so-called polarization phenomenon to approach capacity in arbitrary channels [16].

The polar coding maps the information bits to the $K$ most reliable locations in $u$. The remaining $N - K$ input bits are frozen bits, known to both encoder and decoder. We use $\mathbb{K}$ and $\mathbb{F}$ to denote the subsets of $\{1, 2, \ldots, N\}$ that correspond to the information bit and frozen bit locations, respectively. The lowest reliability can be selected to be in $\mathbb{F}$ for frozen bits, e.g., by Bhattacharyya parameter [16], density evolution [23], [24], Gaussian approximation [25], beta expansion [26], genetic algorithm [27], and deep learning [28].

### B. Polar Decoding

The original SC decoder [16] proceeds sequentially over the bits, from $u_1$ to $u_N$. For each index $i \in \{1, 2, \ldots, N\}$, an estimate $\hat{u}_i$ for bit $u_i$ is made as follows. If $i \notin \mathbb{K}$, then $\hat{u}_i$ is set to the known value of $u_i$, otherwise, when $i \in \mathbb{K}$, $\hat{u}_i$ is set to the most likely value for $u_i$ given the channel outputs, assuming that the previous estimates $[\hat{u}_1, \hat{u}_2, \ldots, \hat{u}_{i-1}]$ are correct. The SC decoding was improved by the SCL decoder [19], which proceeds similarly to the SC decoder, except that for each data bit index $i \in \mathbb{K}$, the decoder retains both possible estimates, $\hat{u}_i = 0$ and $\hat{u}_i = 1$, in subsequent decoding paths. The list-decoding approach limits the number of paths to a fixed-size list $L$ of the most likely partial paths. The combination of SCL decoding with an embedded cyclic redundancy check (CRC) to reject invalid paths yields significantly improved performance [19], [37]. Various other decoding algorithms were proposed in the literature, e.g., simplified SC decoding [29], neural SC decoding [30], and BP list decoding [31].

### C. Computational Complexity

It is known that short LDPC codes do not perform well as shown in [15], where nonbinary (NB) coding can improve LDPC codes in the short-length regimes. However, the computational complexity of NB-LDPC decoding is generally higher than binary counterparts, in particular for large Galois field sizes. It is thus of great importance to realize low computational complexity in addition to high coding gain. We evaluate the computational complexity of polar decoding and show that it is competitive with LDPC decoding.

The polar SCL decoding has a log-linear complexity; specifically, $O[LN \log_2(N)/2]$ for a list size of $L$. This nonlinearity is a major drawback in comparison to the linear complexity of LDPC BP decoding, i.e., $O[2Id_vN]$ where $d_v$ denotes the average degree of variable nodes (VNs). Note that the factor of $2Id_v$ comes from the bidirectional message passing, whereas SCL decoding uses unidirectional message passing over $N \log_2(N)/2$ VNs. Due to the nonlinear complexity, polar codes can eventually be less effective than LDPC codes as we increase the block lengths $N$. However, it turns out to be an advantage when we aim to reduce the block sizes in order to decrease decoding latency. This is illustrated in Fig. 2 where complexity per coded bit (i.e., divided by $N$) is plotted as a function of block length $N$ for polar and LDPC decoding. Because per-bit complexity is constant depending on average degree $d_v$ for LDPC codes, there is no motivation to decrease the block length. In contrast, polar decoding becomes simpler when we reduce block sizes. Remarkably, polar decoding will be more efficient than typical LDPC decoding at short block lengths of $N < 10^4$. This promotes polar codes as a strong candidate for latency-critical systems.

Although the actual computational complexity may vary depending on hardware implementation, most prototyping studies [18] have revealed that polar codes can compete favorably with LDPC codes in terms of complexity. Note that the LDPC decoding is more complicated for higher rates because the average check-node (CN) degree is larger, whereas polar codes have at most three degrees at CNs. Nevertheless, polar SCL decoding is not amenable to parallel implementation. In this paper, we propose a highly parallelizable polar code family whose complexity is $O[LN \log_2(N/Q)/2]$ for a parallelism factor of $Q$. From Fig. 2 we can observe the significant advantage in its decoding complexity. The details of our proposed QC polar codes will be described in the next section.

![Computational Complexity per Coded Bit](image-url)
III. Protograph-Based QC Polar Codes

A. Protograph Codes

Thorpe [6] introduced the concept of protograph codes, a class of LDPC codes constructed from a protograph in such a way that the 1’s in the parity-check matrix are replaced by \((Q \times Q)\)-permutation matrices and the 0’s by \((Q \times Q)\)-zero matrices. The permutation size \(Q\) is also called a lifting size. If the permutation matrices are circulant, the protograph code reduces to a well-known QC LDPC code [7]. To the best of authors’ knowledge, no studies have been reported for designing the protographs for polar codes.

Analogously in lifting operations of the parity-check matrix for LDPC codes, we replace the generator matrix of polar codes. For example, the following generator matrix for 2-stage polar codes is replaced with permutation matrices \(P_{i,j}\):

\[
G^{(2)} = \begin{bmatrix}
1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 \\
\end{bmatrix} \xrightarrow{Lifting} \begin{bmatrix}
P_{1,1} & P_{1,2} & P_{1,3} & P_{1,4} \\
0 & P_{2,2} & 0 & P_{2,4} \\
0 & 0 & P_{3,3} & P_{3,4} \\
0 & 0 & 0 & P_{4,4} \\
\end{bmatrix},
\]

where 0 is an all-zero matrix of size \(Q \times Q\). The simplest choice of permutation matrices is a weight-1 circulant matrix: \(P_{i,j} = I(s^i_{j})\), where \(I(s)\) denotes the \(s\)th circulant permutation matrix obtained by cyclically right-shifting a \(Q \times Q\) identity matrix by \(s\) positions, and \(s^i_{j}\) is a shift value to design. For this special case, we may call the protograph polar codes as QC polar codes. It can be regarded as a generalized low-density generator matrix (LDGM) based on polar codes.

We consider a hardware-friendly lifting operation at each polarization stage with identity diagonal matrices \(P_{i,i} = I(0)\). Our lifting operation is illustrated in Fig.4 where we replicate \(Q\)-parallel polar encoders and permut exclusive-or (XOR) incident bits among the parallel encoders. Fig.1 shows an example of QC polar codes having a shift base matrix of size \(n \times 2^n-1\) as follows:

\[
S = \begin{bmatrix}
139 & 252 & 234 & 156 & 157 & 142 & 50 & 68 \\
134 & 25 & 178 & 20 & 254 & 101 & 146 & 212 \\
79 & 192 & 144 & 129 & 204 & 71 & 237 & 252 \\
37 & 235 & 140 & 72 & 255 & 137 & 203 & 133 \\
\end{bmatrix},
\]

whose \((i,j)\)th shift value is assigned for the \(j\)th polarization unit at the \(i\)th stage. Note that the QC polar codes still hold most benefits of original polar codes such as structured encoding and decoding. As we will discuss below, the QC polar codes have a number of remarkable features.

B. High-Girth Design

In order to achieve good performance, we shall design the shift values of QC polar codes. One obviously poor choice is the case when we use all zeros for shifting, leading to mutually independent \(Q\)-parallel short polar codes without any coupling gain. The protograph codes are often designed to achieve a high girth — the “girth” of a code is the length of the shortest cycle in the code graph. It is known [11] that the girth of any conventional QC LDPC code is upper bounded by 12. Tanner [12] proposed a systematic way to optimize shift values to achieve girth-12. It was further shown in [13] that an irregular QC LDPC code can achieve a girth larger than 12.

For QC polar codes \((2^n, K, Q)\) of code length \(N = 2^nQ\), there are \(n2^{n-1}\) shift values to design as in (2). Unfortunately, the factor graph of polar codes are inherently loopy and there exist a large number of short cycles as illustrated in Fig.3. Nonetheless, by optimizing shift values, we can increase the girth for QC polar codes with \(Q > 1\). For example, the cycle-4 loop in Fig.4(a) can be eliminated if the shift values satisfy the condition [14]:

\[
-s_{1,1} - s_{2,2} + s_{1,2} + s_{2,1} \neq 0 \pmod{Q},
\]

where we accumulate shift values of all proto-CN’s along the loop. Note that the shift values are negated if the path goes downward. This explains the long-lasting problem that the BP decoding performs very poorly for the conventional polar codes \((Q=1)\), i.e., the accumulated shifts will be always zero, resulting in a small girth of 4. Our QC polar codes resolve this issue by maximizing the girth in the protograph. Similarly, the cycle-6 loop in Fig.4(b) can be removed if we can satisfy

\[
-s_{1,3} - s_{3,4} + s_{1,2} + s_{3,1} - s_{2,1} \neq 0 \pmod{Q}.
\]

Note that irregular polar coding [35] is an alternative that could remove some, but not all, short-cycle loops. We extended the greedy design method used for irregular polar coding to jointly
optimize frozen bit locations and circulant shift values by means of protograph extrinsic information transfer (P-EXIT) [8], [9] and a hill-climbing girth maximization [14].

C. Error-Rate Performance

Fig. 5 shows bit-error rate (BER) performance as a function of signal-to-noise ratio (SNR) for short polar codes \((2^n, 2^{n-1}, 2^q)\) with \(n = 2\) polarization stages in additive white Gaussian noise channels. We here use 32-iteration BP decoding with two-way round-robin scheduling from the first to the last stages and its reversed direction alternatingly (parallel flooding updates per stage). The first two bits \([u_1, u_2]\) are frozen. The following shift base matrices are considered:

\[
\begin{bmatrix}
0 & 0 \\
0 & 0 \\
0 & 1 \\
1 & 0
\end{bmatrix}, \quad
\begin{bmatrix}
0 & 1 \\
0 & 0 \\
1 & 0 \\
0 & 1
\end{bmatrix}, \quad
\begin{bmatrix}
0 & 0 \\
0 & 0 \\
1 & 1 \\
-1 & 1
\end{bmatrix}
\]  

(4)

for standard polar codes \((Q = 2^q = 1)\), un-optimized QC polar codes, optimized QC polar codes, and irregular QC polar codes, respectively. We denote a pruned polarization by a negative shift value. As the first two cases do not satisfy the condition in (5) to eliminate girth-4, the BER performance is worse than the other two cases. By eliminating the cycle-4 loop, the QC polar codes can achieve a gain of 0.9 dB without sacrificing any computational complexity. We found that frozen bit locations are also important; specifically, no gain was achieved with \([u_1, u_3]\) being frozen.

The performance improvement can be more significant for a deeper stage \(n\) and larger lifting size \(Q\). We plot the BER performance for half-rate 4-stage QC polar codes \((2^4, 2^3, 2^q)\). We can see that the increase of the lifting size \(Q = 2^q\) can significantly improve performance by up to 2.4 dB gain over the standard polar codes. It should be noted that the per-bit complexity is identical for all of these QC polar codes regardless of the lifting size \(Q\); specifically, \(Q\) parallel decoding of short polar codes requires a total complexity on the order of \(Q \times O[n2^{n-1}]\) for a total codeword length of \(Q \times 2^n\) bits. For \(Q = 256\), our girth design method could remove all short cycles up to 6. The designed shift base matrix is written in (2), and also depicted in Fig. 1.

We next demonstrate that our QC polar codes using shallow polarization stages can compete against long standard polar codes with deeper polarization stages. Fig. 7 shows the BER performance of 16-stage standard polar codes and 6-/8-stage QC polar codes for a total block length of \(N = 2^{16}\) bits. We also present the shallow 6-/8-stage polar codes without protograph lifting. Noticeably, shallow 6-stage QC polar codes with \(Q = 1024\) parallel BP decoding can outperform SC decoding of 16-stage polar codes. Furthermore, our 8-stage QC polar codes with \(Q = 256\) can achieve performance competitive with state-of-the-art SCL decoding (with a list size of \(L = 32\)) for the long 16-stage polar codes. In addition, it was verified that the QC polar codes can resolve the issues of BP decoding to offer comparable performance to SCL.
decoding with large list sizes. These results are practically impactful because the encoding, decoding, and code design of shallower polar codes are much simpler and more efficient.

D. Irregular Pruning

We finally investigate the irregular QC polar codes which deactivate polarization units. As discussed, pruning proto-polarization units may also assist removing short cycles. It was shown in [36] that the conventional irregular polar codes are often capable of reducing the encoding/decoding complexity, decoding latency, and even BER (due to improved Hamming weight distributions). Fig. 8 shows performance of QC polar codes \((2^n,2^{n-1},2^k)\) when proto-polarization units are gradually pruned by a greedy algorithm [36]. For 4-stage polar codes, the performance degrades as the number of inactive polarizations increases. Nevertheless, the QC polar codes with \(Q = 256\) are still better than the standard polar codes \((Q = 1)\) until 64% of the polar units are removed. For 6-stage polar codes with \(Q = 1024\) lifting, it was observed that pruning up to 7% of the proto-polarization units improves the BER performance over the regular counterpart. In consequence, the irregular QC polar codes can further reduce the decoding complexity with potential performance improvement.

E. Discussion

Some major advantages of the proposed protograph polar codes are listed below:

- There is a higher flexibility in codeword lengths of non powers-of-two, i.e., \(N = 2^nQ\).
- Irregular polarization is straightforward to apply with the shift value matrix design.
- Well-established techniques such as girth design and P-EXIT from LDPC codes are applicable.

We however found that the recent BP list decoding [31] was not compatible with the QC polar codes as it is. As we focused on the proof-of-principle study in this paper, there remain many research directions, including extensions to BP list decoding, systematic encoding, nonbinary codes, systematic circulant shift design, BP scheduling optimization, and multi-weight permutation. In particular, it is interesting to consider inhomogeneous polar codes, e.g., non-identical frozen bit locations across \(Q\) polar codes, and circulant permutations among different polarization stages. We also note that our QC polar codes are similar to polar product codes [41] in the sense that parallel short polar codes are coupled, but the fundamental difference lies in its mechanism of coupling (QC polar codes do not need additional row/column polar codes but computation-free circulant). Also, mixture-kernel and nonbinary polar codes are analogous to the QC polar codes in the sense that a single polarization unit processes multiple bits at once in parallel. However, nonbinary polar codes require additional complexity and there is a limited flexibility to choose a Galois field size \(Q\). More importantly, \(Q\)-ary polar codes have only \(\log_2(Q)\) bits parallelism, whereas fully \(Q\)-parallel encoding is possible in the QC polar codes. We believe that the protograph design for generalized LDGM (including QC polar codes) will stimulate the research community.

IV. CONCLUSIONS

We proposed a novel class of polar codes called QC polar codes, which replicate parallel short polar encoders and decoders with circulant permutations to exchange intermediate messages among them. We developed a protograph-based design method to optimize the girth to achieve high coding gain. By removing short cycles, the proposed QC polar codes can outperform the standard polar codes. We believe that the QC polar coding offers a breakthrough to resolve the long-standing issue that BP decoding performs poorly for conventional polar codes due to the inherent girth-4. It was demonstrated that the QC polar codes with shallow polarization can achieve the state-of-the-art performance of deeper polar codes at a considerably reduced complexity. The QC polar codes are hardware friendly as highly parallel encoding/decoding is feasible with a reduced polarization stage. We also evaluated the impact of irregular QC polar codes, which can further decrease the complexity and BER for some cases. For the proposed protograph codes, we addressed a number of interesting extensions for future research directions.

ACKNOWLEDGMENT

We would like to thank Drs. David S. Millar, Keisuke Kojima, and Kieran Parsons at MERL for their useful discussion.
