Non-Binary Polar Codes for Spread-Spectrum Modulations

Valentin Savin, CEA-LETI, Université Grenoble Alpes, France (valentin.savin@cea.fr)

Abstract—This paper proposes a new coded modulation scheme for reliable transmission of short data packets at very low signal-to-noise ratio, combining cyclic code shift keying modulation and non-binary polar coding. We consider non-binary polar codes defined over Galois fields, and propose a new design methodology, aimed at optimizing the choice of the kernel coefficients. Numerical results show that the system performance is close to the achievable limits in the finite blocklength regime.

I. INTRODUCTION

Recent years have seen an explosive growth in the number of devices connected and controlled by the Internet. The wide range of applications for Internet of Things (IoT) technology is usually divided into two use-cases, known as either “critical IoT” or “massive IoT”. The latter is characterized by a high density of connected devices, small data payloads, and low sensitivity levels, due to stringent constraints on the device energy consumption and cost. Maximizing the spectral efficiency of an IoT network is a key prerequisite for providing massive connectivity. Yet, the first wave of IoT standards are close to the achievable limits in the finite blocklength regime.

The paper is organized as follows. In Section II we introduce the system model and derive the achievable rates in the both asymptotic and finite blocklength regimes. In Section III we shortly discuss non-binary polar coding, and present non-binary polar codes defined over Galois fields. In Section IV we present the non-binary code design methodology, aimed at optimizing the choice of the kernel coefficients. Numerical results are presented in Section V.

II. SYSTEM MODEL

A. CCSK Modulation

We denote by \( \mathcal{U} \triangleq \{0, 1, \ldots, q - 1\} \) the set of integers comprised between 0 and \( q - 1 \), where \( q = 2^p \) is a power of 2. We shall further identify \( \mathcal{U} \cong \mathbb{Z}_q \triangleq \{0, 1\}^p \), by identifying an integer to its binary representation, \( u \cong (u(0), \ldots, u(p-1)) \).

Let \( \mathbf{P}_u \triangleq (\mathbf{P}_0(0), \mathbf{P}_0(1), \ldots, \mathbf{P}_0(q-1)) \) be a pseudo-random noise (PN) sequence, of length \( q \), with good cross-correlation properties (e.g. \( \mathbf{P}_0 \) may be generated by a linear feedback shift register, with primitive feedback polynomial). We assume that \( \mathbf{P}_0(i) \in \{-1, +1\}, \forall i = 0, \ldots, q - 1 \). For \( u \in \mathcal{U} \), we define \( \mathbf{P}_{u} \) to be the sequence obtained by shifting \( \mathbf{P}_0 \) circularly to the left, by \( u \) positions, that is

\[
\mathbf{P}_u(i) \triangleq \mathbf{P}_0(i + u \mod q), \forall i = 0, \ldots, q - 1. \tag{1}
\]

The CCSK modulation maps an element \( u \in \mathcal{U} \) to the sequence \( \mathbf{P}_u \). The ratio \( p/q \) is referred to as the spreading factor of the modulation.

B. Demodulation

We will use the following notation.

- \( \mathbf{U} = (\mathbf{U}(0), \ldots, \mathbf{U}(p-1)) \) denotes a uniform random variable, with values in \( \mathcal{U} \). Realizations of a \( \mathbf{U} \) represent unmodulated symbols (input to the CCSK modulation).
- \( \mathbf{X} = (\mathbf{X}(0), \mathbf{X}(1), \ldots, \mathbf{X}(q-1)) \in \{-1, +1\}^q \) denotes the random variable defined by modulating \( \mathbf{U} \). Hence, \( \mathbf{X} = \mathbf{P}_u \Leftrightarrow \mathbf{U} = u \).
- \( \mathbf{Y} = (\mathbf{Y}(0), \mathbf{Y}(1), \ldots, \mathbf{Y}(q-1)) \in \mathbb{R}^q \) denotes the received signal.
- \( \mathbf{Y} = (\mathbf{\tilde{Y}}(0), \mathbf{\tilde{Y}}(1), \ldots, \mathbf{\tilde{Y}}(q-1)) \in \mathbb{R}^q \), where

\[
\mathbf{\tilde{Y}}(i) \triangleq \log \frac{\Pr(X(i) = +1 \mid Y(i))}{\Pr(X(i) = -1 \mid Y(i))} \tag{2}
\]

Assuming that the CCSK modulated signal \( \mathbf{X} \) undergoes real additive white Gaussian noise, we have

\[
\mathbf{Y}(i) = \mathbf{X}(i) + Z(i) \quad \text{and} \quad \mathbf{\tilde{Y}}(i) = \frac{2}{\sigma^2} Y(i), \tag{3}
\]
where $Z(i)$ are real-valued, mutually independent, normal random variables, with mean 0 and variance $\sigma^2$.

Given the received signal $Y$, the symbol-level Log-Likelihood Ratio (LLR) values are defined by

$$\Gamma(u) \triangleq \log \frac{\Pr(U = 0 \mid Y)}{\Pr(U = u \mid Y)}, \quad \forall u \in \mathcal{U} \quad (4)$$

Hence, we have

$$\Gamma(u) = \log \frac{\Pr(U = 0 \mid Y)}{\Pr(U = u \mid Y)} = \log \frac{\Pr(X = P_0 \mid Y)}{\Pr(X = P_u \mid Y)}$$

$$= \sum_{i=0}^{q-1} \log \frac{\Pr(X(i) = P_0(i) \mid Y(i))}{\Pr(X(i) = P_u(i) \mid Y(i))} \quad (5)$$

$$= \sum_{i=0}^{q-1} \frac{1}{2} \log \frac{\Pr(X(i) = +1 | Y(i))}{\Pr(X(i) = -1 | Y(i))} \quad (6)$$

$$= \frac{1}{2} (\tilde{Y} \cdot P_0 - \tilde{Y} \cdot P_u) \quad (7)$$

where $\tilde{Y} \cdot P \triangleq \sum_i \tilde{Y}(i) P(i)$ denotes the usual dot product of sequences (vectors) $\tilde{Y}$ and $P$. Since $P_u$ is a circular shifted version of $P_0$, dot products $Y \cdot P_u$, $u \in \mathcal{U}$, can be conveniently computed by using the discrete Fourier transform, denoted by $\mathcal{F}$. Precisely,

$$Y \cdot P_u = (Y * P_0)(u) = \mathcal{F}^{-1}(\mathcal{F}(Y)^* \cdot \mathcal{F}(P_0))(u), \quad (9)$$

where $\mathcal{F}(Y)^*$ is the complex conjugate of $\mathcal{F}(Y)$. Finally, from the above LLR values, the probability distribution of $U$ conditional on $Y$ can be computed by

$$\Pi(u) \triangleq \Pr(U = u \mid Y) = \frac{e^{-\Gamma(u)}}{\sum_{u' \in \mathcal{U}} e^{-\Gamma(u')}} \quad (10)$$

In case that the unmodulated symbols are encoded by a non-binary code, the received signal is first demodulated, then the symbol-level LLR values (or equivalently, the corresponding probability distribution on the alphabet $\mathcal{U}$) are supplied to the non-binary decoder.

### C. Achievable Rates

We assume that the unmodulated symbols are encoded by a non-binary code, with alphabet $\mathcal{U}$. The coding rate is the ratio between the number of source symbols and the total number of encoded symbols.

**Asymptotic Blocklength Regime:** By Shannon’s noisy-channel coding theorem [9], the maximum achievable (coding) rate, denoted in the sequel by $R$, is given by mutual information between the input $U$ of the CCSK modulation and the output $Y$ of the channel

$$R \triangleq I(U; Y) = H(U) - H(U|Y), \quad (11)$$

where $H$ denotes the Shannon entropy. We assume a base-$q$ logarithm for the entropy, such that $R \in [0, 1]$. Since the channel is symmetric, its capacity is achieved for an uniformly distribution input $U$. Hence, we have $H(U) = 1$, while the conditional entropy $H(U|Y)$ can be conveniently estimated numerically, by averaging over the channel output $Y$,

$$H(U|Y) = E_Y \left[ -\sum_{u \in \mathcal{U}} \Pi(u) \log_q \Pi(u) \right]. \quad (12)$$

**Finite Blocklength Regime:** In the non-asymptotic regime, the backoff from channel capacity can be accurately characterized by a parameter known as channel dispersion [10]. Specifically, the maximum achievable coding rate can be tightly approximated by

$$R^* \triangleq R - \sqrt{\frac{V}{N}} Q^{-1}(\varepsilon), \quad (13)$$

where $R$ is the channel capacity, and $V$ is the channel dispersion. $R^*$ is usually referred to as the normal approximation. Using [10, Theorem 49], the channel dispersion parameter can be computed as

$$V = H_2(U \mid Y) - H(U \mid Y)^2, \quad (14)$$

where $H_2(U \mid Y) \triangleq E_Y \left[ -\sum_{u \in \mathcal{U}} \Pi(u) \log_q^2 \Pi(u) \right], \quad (15)$

which can again be be conveniently estimated numerically by Monte-Carlo simulation.

### III. Non-Binary Polar Codes

Two main approaches have been proposed in the literature for polarizing channels with non-binary input alphabets. The first one relies on using higher-dimensional non-binary kernels, that is, kernels of size $\ell \times \ell$, with $\ell > 2$ [4–6]. Such an approach is characterized by an increased complexity, due to both the size of the non-binary alphabet, and the higher kernel dimension. A different approach, proposed in [3], is to use a randomized construction, based on the original kernel proposed by Arikan. Precisely, the kernel transformation is defined by $(u_0, u_1) \mapsto (u_0 \oplus u_1, \pi(u_1))$, where $\pi$ is a random permutation of the non-binary alphabet (here ‘$\oplus$’ may be any additive group operation on the non-binary alphabet). Channel polarization essentially states that for a random choice of permutations throughout the recursive channel combining and splitting procedure, the synthesized virtual channels polarize to either useless or perfect channels. In this case, the polar code construction encompasses the choice of both channel combining permutations and virtual channels used to transmit information symbols. Of course, once the code is constructed, randomness does no longer exist, and the complexity of polar code encoding and decoding is essentially the same as for the Arikan’s kernel.

The non-binary polar codes considered in this work are based on the randomized construction described above. However, we consider non-binary polar codes defined over Galois fields (GF), and rather than random GF permutations, we consider linear permutations defined by the multiplication with a non-zero GF element [7, 8]. Precisely, using the notation from the previous section, we denote by $W(Y \mid U)$ the channel with non-binary input alphabet $\mathcal{U}$, encompassing both the CCSK modulation and the actual transmission channel. We further endow $\mathcal{U}$ with a GF structure, with (additive, multiplicative) operations denoted by $(\oplus, \cdot)$. Finally, the kernel transformation, illustrated in Fig. I is defined by $(u_0, u_1) \mapsto (v_0, v_1) \triangleq (u_0 \oplus u_1, h \cdot u_1)$, where $h \in \mathcal{U}^*$ (the multiplicative group of non-zero GF elements), referred to as kernel coefficient.
Throughout the rest of the paper, we denote by $GF(q)$ the Galois field with $q$ elements, and further identify $U \cong GF(q)$.

### A. Optimization of the kernel coefficients

While the polarization result in [3], [7] essentially states that a random choice of the kernel coefficients is good enough, it might not be optimal. Thus, the optimization of the kernel coefficients is aimed at accelerating the speed of polarization of the synthesized virtual channels. There are three parameters that may be used to describe the polarization process: the mutual information, the Bhattacharyya parameter, and the error probability of the synthesized virtual channels. The former approaches 0 (respectively 1) if and only if the latter two approach 1 (respectively, 0). Any of these parameters may be used within the proposed optimization procedure, and for the moment we shall simply use polarizing parameter to refer to any of them. To accelerate the speed of polarization, we choose the kernel coefficients so as to maximize the difference between the polarizing parameters of the bad and good channels synthesized by the channel combining and splitting procedure.

The optimization procedure is illustrated at Fig. 2 for a polar code of length $N = 8$, corresponding to $n = 3$ polarization steps. The original non-binary channel is denoted by $W$. We denote by $W^{(0)}$ and $W^{(1)}$ the bad and good channels, respectively, after one step of polarization. Then, for $n > 0$, we define recursively

$$W^{(i_1 \ldots i_n)} := \left(W^{(i_1 \ldots i_{n-1})}\right)^{\Pi_{i_n}}, \forall (i_1, \ldots, i_n) \in \{0, 1\}^n$$

In Fig. 2 we have indicated on each horizontal wire the virtual channel $W^{(i_1i_2\ldots)}$ “seen” by the corresponding symbol throughout the polarization process. All the kernels on the first (right-most) polarization step combine two copies of the $W$ channel. Therefore, only one coefficient needs to be optimized, denoted by $h_0$. We define $h_0$ as

$$h_0 := \arg\max_{h \in GF(q)} \left| P^{(0)}(h) - P^{(1)}(h) \right|,$$

where $P^{(0)}(h)$ and $P^{(1)}(h)$ denote the polarizing parameters of $W^{(0)}$ and $W^{(1)}$ channels, respectively, assuming that the channel combining coefficient is equal to $h$. We numerically estimate the values of $P^{(0)}(h)$ and $P^{(1)}(h)$, for all $h \in GF(q) \setminus \{0\}$, based on Monte Carlo simulation (see also Section IV-C).

Once the value of $h_0$ is determined, we can optimize the kernel coefficients for the second (middle) polarization step. There are two different types of kernels on the second polarization step, combining either two copies of $W^{(0)}$, or two copies of $W^{(1)}$. Therefore, two coefficients need to be optimized, denoted by $h_1$ and $h_2$ in Fig. 2. Hence, we define

$$h_1 := \arg\max_{h \in GF(q)} \left| P^{(0)}(h) - P^{(1)}(h) \right|,$$

$$h_2 := \arg\max_{h \in GF(q)} \left| P^{(1)}(h) - P^{(1)}(h) \right|,$$

where $P^{(i_1i_2)}(h)$ denotes the polarizing parameters of the $W^{(i_1i_2)}$ channel, assuming the channel combining coefficient on the second polarization step is equal to $h$. The value of $P^{(i_1i_2)}(h)$ is again estimated numerically through Monte Carlo simulation. Then the optimization process continues recursively, until the desired number of polarization steps is reached.

### B. Non-binary polar decoding

We first consider the decoding of a non-binary channel, which is illustrated at Fig. 3. As before, let $u_0, u_1 \in GF(q)$ denote the kernel inputs, and $v_0, v_1 \in GF(q)$ denote the kernel outputs. Decoding operates in the opposite direction, i.e., it takes as inputs $\Pi_V^{(0)}$ and $\Pi_V^{(1)}$, the probability distribution functions (PDFs) of $v_0$ and $v_1$, respectively, and outputs $\Pi_U^{(0)}$ and $\Pi_U^{(1)}$, the PDFs of $u_0$ and $u_1$, respectively. It can be easily seen that $\Pi_U^{(0)}$ and $\Pi_U^{(1)}$ can be computed from $\Pi_V^{(0)}$ and $\Pi_V^{(1)}$, by the following formulas:

$$\Pi_U^{(0)}(u) = \sum_{u' \in GF(q)} \Pi_V^{(0)}(u \oplus u') \Pi_V^{(1)}(h \cdot u'),$$

$$\Pi_U^{(1)}(u) = \eta \Pi_V^{(0)}(u_0 \oplus u) \Pi_V^{(1)}(h \cdot u),$$

where $\eta$ is a normalization factor, determined such that $\sum_{u \in GF(q)} \Pi_U^{(1)}(u) = 1$. In equation (21), the computation of $\Pi_U^{(1)}(u)$ requires the knowledge of $u_0$. Such a decoder is referred to as genie-aided, and it is used at the code design stage. For a real-world decoder, used to decode a codeword transmitted over a noisy channel, equation (21) is replaced by

$$\Pi_U^{(1)}(u) = \eta \Pi_V^{(0)}(u_0 \oplus u) \Pi_V^{(1)}(h \cdot u),$$
where either $\hat{u}_0 = u_0$ if the latter is known (frozen bad channel), or $\hat{u}_0 = \arg \max_{u \in GF(q)} \Pi_U^{(0)}(u)$ is the estimate of $u_0$, otherwise.

The successive cancellation (SC) decoder (either genie-aided or real-world) uses the above kernel decoding rules in a recursive manner, so as to propagate the PDFs of the transmitted symbols from the right-hand side (transmission channel side) to the left-hand side of the polar graph. There is one such a recursion for each $W^{(i_1 \ldots i_n)}$ channel (deriving from the recursive definition of the channel), which are then decoded successively.

C. Choice of the polarizing parameter and code construction

Since we are interested on the error rate performance of the constructed polar code, we take the polarizing parameter used within the optimization procedure (from Section IV-A) to be the error probability of the synthesized virtual channels. An efficient way to numerically estimate the error probability of the synthesized virtual channels is described below, where $u^{(i_1 \ldots i_n)} \in GF(q)$ denotes the input of the $W^{(i_1 \ldots i_n)}$ virtual channel, $(i_1 \ldots i_n) \in \{0,1\}^n$.

1) Randomly generate a set of inputs $\{u^{(i_1 \ldots i_n)} : (i_1 \ldots i_n) \in \{0,1\}^n\}$, encode them, and transmit the obtained codeword over the non-binary channel.
2) Run the genie-aided SC decoder to determine the PDFs of the virtual channels’ inputs $u^{(i_1 \ldots i_n)}$, denoted by $\Pi_U^{(i_1 \ldots i_n)}$.
3) Hence, the one-run error probability $P^{(i_1 \ldots i_n)}$ is given by $P^{(i_1 \ldots i_n)} = 1 - \Pi_U^{(i_1 \ldots i_n)}(u^{(i_1 \ldots i_n)})$. 
   (c) Repeating the steps 1–3 many times, the error probability of the virtual channel $W^{(i_1 \ldots i_n)}$ is estimated by taking the average of the one-run error probability:

$$P^{(i_1 \ldots i_n)} = E[P^{(i_1 \ldots i_n)}]$$

The above procedure is used recursively within the optimization procedure from Section IV-A, to optimize the kernel coefficients at the different polarization steps. Moreover, once the optimization procedure completed, we may use the $P^{(i_1 \ldots i_n)}$ values to sort the virtual channels from the best (lowest error probability) to the worst (higher error probability) one, and then use the best channels to transmit information symbols. This completes the polar code construction, as we have made a choice of the kernel coefficients, and determined the virtual channels to use for transmitting information symbols. Moreover, when the polar code construction completes, we also get an estimate the SC decoding error probability, denoted WER$_{SC}$. To simplify the notation, let us denote by $p^{(1)}, \ldots, p^{(K)}$ the error probability of the $K$ virtual channels carrying information symbols. Then, we have

$$\text{WER}_{SC} := 1 - \prod_{k=1}^{K} (1 - p^{(k)})$$

For binary polar codes, WER$_{SC}$ is known to provide a tight upper-bound on the word error rate (WER) performance of the SC decoder (which also explains the notation). In Section V we will show that the same is true for non-binary polar codes.

V. Numerical Results

We assume that non-binary coded symbols in GF($q = 2^p$) are mapped into CCSK symbols of length $q$, which then undergo real-valued additive white Gaussian noise. The signal to noise ratio (SNR) value is defined as $\text{SNR} = -10 \log_{10}(\sigma^2)$, where $\sigma^2$ is the noise variance. We have considered SNR values from $-25$ to $-5$ dB, with a step of 0.5 dB, and for each SNR value we have constructed non-binary polar codes with parameters given in Table I. Recall that $n$ is the number of polarization steps, $N = 2^n$ is the non-binary code length (number of coded symbols), $N_p$ is the binary code length (number of coded bits), and $N_q$ is the effective number of transmitted bits (after CCSK modulation). The number of information bits, denoted $K_{\text{bin}}$, depends on the coding rate, and can be obtained by $K_{\text{bin}} = RN_p$. We shall also refer to $R$ as the native coding rate, and define the effective coding rate $R_{\text{eff}} = \Delta pR/q$, so that to take into account the spreading factor of the CCSK modulation.

Fig. 4 shows the WER performance for various native coding rate values $R$, varying from 1/48 to 9/10. Two WER curves are shown for each native coding rate, a solid one, corresponding to Monte Carlo simulation results, and a dashed one, corresponding to the WER estimated at the code construction stage (Section IV-C). It can be observed that the WER estimates we obtain at the code construction stage are tight. Fig. 5 shows the achievable native and effective coding rates, for a target WER = 10$^{-4}$. The figure shows the achievable coding rates for different Galois fields, obtained by using either the WER estimates at the code construction stage (dashed curves), or the WER obtained by Monte Carlo simulation (superimposed full markers). Moreover, dashed-dotted curves show the normal approximation of the maximum achievable rate in the finite block-length regime, while solid curves show the maximum achievable rate in the asymptotic block-length regime. It can be seen that the gap between the achievable coding rates under non-binary polar coding and the normal approximation bound is about 1 – 1.5 dB.

| $p$ | $n$ | $N_p$ | $N_q$ |
|-----|-----|-------|-------|
| 6   | 10  | 1024  | 6144  |
| 8   | 8   | 256   | 2048  |
| 10  | 6   | 64    | 640   | 65536 |
VI. CONCLUSION

This paper investigated a new approach to reliable transmission of short data packets at very low signal-to-noise ratio, which combines CCSK modulation and non-binary polar coding. We proposed a design methodology for the non-binary polar code, aimed at accelerating the polarization speed, though maximizing the difference between the polarizing parameters of the synthesized virtual channels. The proposed methodology is generic and may be used for other applications. Numerical results show that the system performance is close to the achievable limits in the finite blocklength regime. We expect that the observed performance may be further improved, by using a more powerful SC-List decoder [8].

REFERENCES

[1] O. Abassi, L. Conde-Canencia, M. Mansour, and E. Boutillon, “Non-binary coded CCSK and frequency-domain equalization with simplified LLR generation,” in International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2013, pp. 1478–1483.

[2] K. Saied, A. C. Al Ghouwayel, and E. Boutillon, “Quasi cyclic short packet for asynchronous preamble-less transmission in very low SNRs,” https://hal.archives-ouvertes.fr/hal-02884668, 2020.

[3] E. Şaşoğlu, E. Telatar, and E. Arikan, “Polarization for arbitrary discrete memoryless channels,” in IEEE Information Theory Workshop, 2009.

[4] R. Mori and T. Tanaka, “Channel polarization on q-ary discrete memoryless channels by arbitrary kernels,” in IEEE International Symposium on Information Theory, 2010, pp. 894–898.

[5] ——, “Non-binary polar codes using reed-solomon codes and algebraic geometry codes,” in IEEE Information Theory Workshop, 2010, pp. 1–5.

[6] E. Şaşoğlu, “Polar coding theorems for discrete systems,” Ph.D. dissertation, EPFL, Lausanne, Switzerland, 2011.

[7] M.-C. Chiu, “Non-binary polar codes with channel symbol permutations,” in Int. Symp. on Info. Theory and its Applications (ISITA), 2014.

[8] P. Yuan and F. Steiner, “Construction and decoding algorithms for polar codes based on 2 × 2 non-binary kernels,” in Int. Symposium on Turbo Codes & Iterative Information Processing (ISTC), 2018, pp. 1–5.

[9] C. E. Shannon, “A mathematical theory of communication,” Bell System Technical Journal, vol. 27, no. 3-4, pp. 379–423 and 623–656, 1948.

[10] Y. Polyanskiy, H. V. Poor, and S. Verdú, “Channel coding rate in the finite blocklength regime,” IEEE Transactions on Information Theory, vol. 56, no. 5, pp. 2307–2359, 2010.