

Rate-Adaptive Cyclic Complex Spreading Sequence for Non-Binary Decoders

Cédric Marchand, Alexandru-Liviu Olteanu, E. Boutillon

► To cite this version:

Cédric Marchand, Alexandru-Liviu Olteanu, E. Boutillon. Rate-Adaptive Cyclic Complex Spreading Sequence for Non-Binary Decoders. 12th International Symposium on Topics in Coding (ISTC 2023), IEEE, Sep 2023, Brest, France. hal-04192391

HAL Id: hal-04192391 https://hal.science/hal-04192391v1

Submitted on 31 Aug 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers. L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Rate-Adaptive Cyclic Complex Spreading Sequence for Non-Binary Decoders

Cédric Marchand, Alexandru-Liviu Olteanu, Emmanuel Boutillon, Université Bretagne Sud, Lab-STICC UMR 6285, CNRS Email: {emmanuel.boutillon, alexandru.olteanu, cedric.marchand}@univ-ubs.fr

Abstract—This paper presents rate-adaptive spreading sequences for Non-Binary (NB) decoders. The sequence's rateadaptive property enables matching the data rate to the channel conditions. It is obtained by truncating codewords of a cyclic code shift keying (CCSK) sequence while keeping the NB decoder optimized at a fixed code rate. Each chip of the sequence is mapped to a q-ary constellation. The paper presents q-PSK sequence construction processes giving bi-orthogonal codewords at different levels of puncturing. Considering a 256-QAM CCSK modulation and 120 bits payload, the spectral efficiency range is from 0.02 to 6 bits/s/Hz for an SNR range from -15.5 dB to 20 dB, with better FER performance than 5G for all SNR values.

Index Terms—Rate-adaptive, Non-Binary decoder, Spreading sequence, CCSK, puncturing, serial concatenation.

I. INTRODUCTION

Non-Binary (NB) codes are error-correcting codes designed over the Galois Field (GF) of size q, denoted as GF(q), with q > 2 elements. NB-LDPC codes, NB turbo codes, NB turbo product codes, and NB polar codes are known examples of Non-binary codes. These codes have excellent error correction performance, especially for short to medium-length frames [1]. Moreover, when the GF(q) symbols are directly mapped into a q-ary modulation, there is no loss of information during the demapping process. In contrast, binary codes mapped on q-ary modulation suffers from binary marginalization [2]. NB-LDPC codes are standardized in [3] and are used as NB-code in this article without loss of generality. Cyclic Code Shift Keying (CCSK) modulation [4] is a $q = 2^m$ -ary direct-sequence spread spectrum (DSSS) technique that associates *m*-bits symbols to q-chips sequences. The i^{th} CCSK sequence \mathbf{G}_i is derived from the binary root sequence (G) by a left circular shift of G by *i* positions. Then, the sequence is transmitted using binary phase-shift keying (BPSK) modulation.

Combining an NB decoder with CCSK modulation consists of mapping the encoded symbols of the NB encoder onto CCSK sequences. This combination efficiently targets low and very low SNRs. An application is the Quasi-Zenith Satellite System (QZSS) [5], where the encoded 8-bit symbols of a Reed-Solomon (255,223) code are mapped on CCSK sequences.

In [6], the authors proposed to use a truncated CCSK (TCCSK) sequence [4] as an inner code to obtain a rateadaptive code with excellent performance on an extensive range of spectral efficiencies. For example, [6] reports a TCCSK coding scheme with spectral efficiencies ranging from 1/32 to 2/3 bit/s/Hz. Let p be the size of the TCCSK sequence.



Fig. 1. Inner q-ary Truncated CCSK associated with NB encoder

When p < m, there are only 2^p distinct binary sequences to encode 2^m GF symbols. It prevents distinguishing between some symbols, reducing the decoding performance of the overall system.

To overcome this problem, we propose to replace the binary sequence with q-ary phase-shift keying (PSK) sequence, i.e., a sequence of complex symbols that belong to the unit circle. This modification allows generating of distinct sequences, even when p is as small as one.

The paper is organized as follows: Section II introduces TCCSK modulation and the distance metric. Section III presents the methods for constructing the sequences. Section IV presents simulation results and discussions. Finally, Section V concludes the paper.

II. TCCSK MODULATION

A. TCCSK modulation

The binary TCCSK is first described in [4] and then combined with an NB-LDPC code in [6]. The combination comprises a serial concatenation of an outer and inner code, as shown in Fig. 1. The outer code is a Non-Binary code over the Galois Field of order $q = 2^m$ GF(q). At the input, km bits (thus k GF(q) symbols) are encoded by a Non-Binary code to generate n GF(q) symbols, with n > k. The rate of the outer code is $r_o = k/n$. The inner code then encodes each symbol of the GF(q) codeword. The inner code is a code of very low cardinality that contains only q codewords, where each codeword is defined by a distinct circular rotation of a given sequence $\mathbf{G} = (G(0), G(1), ..., G(q - 1))$ of length q. In the sequel, each element $a \in \mathrm{GF}(q)$ is represented by an integer value between 0 and q - 1. The inner code encoding process of a symbol a consists in mapping a to a codeword sequence G_a of length-q, where G_a is the circular left shift rotation of G by a positions.

The inner code is known in the literature as the CCSK modulation. When $G(i) \in \{-1, 1\}$, the CCSK sequence is said binary, and each $G_a(i)$ chip is modulated using BPSK modulation. When G(i) can take more than 2 values, the CCSK sequence is said non-binary.

The CCSK truncation process [4], [6] transmits only the first p chips, $p \leq q$ of the CCSK sequence as shown in Fig. 1. The TCCSK sequence associated with $a \in GF(q)$ is defined as \mathbf{G}_{a}^{p} . With m bits spread on p chips, the overall spectral efficiency s_{e} is defined as

$$s_e = r_o \times \frac{m}{p}$$
 bits/s/Hz. (1)

B. Normalized Minimum Square Distance

The minimum Euclidean distance of a code is a well-known metric to prove the efficiency of a code. We describe this metric applied to the NB-TCCSK modulation. Let \mathbf{G}_{a}^{p} and \mathbf{G}_{b}^{p} be two codewords of the inner code. The square distance $d(\mathbf{G}_{a}^{p}, \mathbf{G}_{b}^{p})^{2}$ between the two codewords is defined as

$$d(\mathbf{G}_{a}^{p}, \mathbf{G}_{b}^{p})^{2} = \sum_{i=0}^{p-1} (\mathbf{G}_{a}^{p}(i) - \mathbf{G}_{b}^{p}(i))^{2}$$
(2)

Considering complex values on the unit circle, $\mathbf{G}_a^p(i)^2 = 1$, and (2) can be simplified to

$$d(\mathbf{G}_{a}^{p}, \mathbf{G}_{b}^{p})^{2} = 2p - 2\mathcal{R}(\langle \mathbf{G}_{a}^{p}, \mathbf{G}_{b}^{p} \rangle).$$
(3)

where $\langle x, y \rangle$ represents the complex scalar product of x and y, and $\mathcal{R}(x)$ represents the real part of x. From (2), it is possible to define the minimum square distance (MSD) of the length-p truncated inner code $D(\mathbf{G}^p)$ as

$$D(\mathbf{G}^p) = \min_{a,b \in \mathrm{GF}(q), a \neq b} \{ d(\mathbf{G}^p_a, \mathbf{G}^p_b)^2 \}.$$
 (4)

The normalized MSD (NMSD) $\overline{D}(\mathbf{G}^p)$ is defined as

$$\bar{D}(\mathbf{G}^p) = \frac{D(\mathbf{G}^p)}{p}.$$
(5)

From (3), (4), and (5), we can deduce that

$$\bar{D}(\mathbf{G}^p) = 2 - \frac{2}{p} \times \max_{a,b \in \mathrm{GF}(q)^2, a \neq b} \{ \mathcal{R}(\langle \mathbf{G}^p_a, \mathbf{G}^p_b \rangle \}.$$
 (6)

Considering a constant amplitude zero auto-correlation (CAZAC) sequence \mathbf{Z} , its cyclically shifted versions are orthogonal to one another, i.e., $a \neq b$ implies $\langle \mathbf{Z}_a^q, \mathbf{Z}_b^q \rangle = 0$. Thus, according to (6), the CAZAC sequence gives $\overline{D}(\mathbf{Z}^q) = 2$. The Zadoff-Chu (ZC) sequence [7], [8] is a well-known CAZAC sequence. Fig. 2 shows the NMSD of sequences as a Function of p. The binary extended maximum-length sequence (EMLS) defined in [6] is compared with the length q = 64 ZC sequence \mathbf{Z} defined as



Fig. 2. Comparison of the evolution of \overline{D} as a function of p for 4-cusps, 64-QAM, EMLS and Zadoff-Chu sequences, with q = 64.

$$Z(i) = e^{2\pi j \frac{i^2}{64}}, \ i = 0, 1, \dots, 63.$$
(7)

Fig. 2 calls for a number of comments. First, when p = q, one can check that the NMSD of the ZC sequence is equal to two. Second, for small values of p, the NMSD of the binary sequence is equal to 0, while it is not the case for the ZC sequence. Last but not least, there is a large span of median values of p (from p = 6 to p = 50) where the NMSD of the binary sequences is significantly greater than the NMSD of the ZC sequence. The question arises if it is possible to generate other sequences that outperform both the ZC and the binary sequences.

III. NB-CCSK SEQUENCE CONSTRUCTION FOR EFFICIENT TRUNCATION

A. q-PSK constellation

In the sequel, we consider the construction of sequence **G** of length q based on chips in the ordered set $C = \{e^{2\pi j \frac{i}{q}}\}_{i=0,1,\ldots,q-1}$. The q chips of the sequence **G** are defined as a bijection with the q elements of the constellation C to guarantee the uniqueness of each point. This bijection can be expressed as a permutation φ that associates to the i^{th} element G(i) of the sequence **G**, the j^{th} element C(j) of the ordered set of constellation point C, with $j = \varphi(i)$.

B. Description of the optimization problem

In Fig. 1, the n = 12 symbols of a codeword are encoded with the sequence **G** defined by the permutation $\varphi = (0, 1, 6, 7, 4, 5, 2, 3)$. The truncation length is set to p = 3, so the first symbol α^0 will be associated to the length-3 sequence \mathbf{G}_0^3 of 8-PSK chips $(e^{0 \times \frac{2j\pi}{8}}, e^{1 \times \frac{2j\pi}{8}}, e^{6 \times \frac{2j\pi}{8}})$. This sequence is indicated by the two arrows on the unit circle in the bottom-right corner of the figure. Similarly, the second symbols α^3 is associated to the length-3 sequence \mathbf{G}_3^3 of 8-PSK chips $(e^{7 \times \frac{2j\pi}{8}}, e^{4 \times \frac{2j\pi}{8}}, e^{5 \times \frac{2j\pi}{8}})$ (not shown in the figure). The concatenation of n = 12 length-3 truncated sequences forms the modulated frame.



Fig. 3. Permutation of an 8-PSK NB-CCSK sequence



Fig. 4. NMSD as a function of φ and p of the 8-PSK NB-CCSK sequence.

Fig. 3 a) illustrates a polar representation of the sequence **G** truncated to p = 2 mapped on an 8-PSK modulation with the identity permutation, i.e., $\varphi_a = Id = (0, 1, 2, 3, 4, 5, 6, 7).$ The arrow numbered 0 illustrates the truncated sequence $\mathbf{G}_0^2 = (0, 1)$, the arrow 1 illustrates the truncated sequence $\mathbf{G}_1^2 = (1,2)$, and so on. The square distance $d(\mathbf{G}_0^2,\mathbf{G}_1^2)^2$ is given by (2) as $2(2-\sqrt{2}) = 1.1716$. One can verify that $\overline{D}(\mathbf{G}_2) = 2 - \sqrt{2}$, and more generally, that $\overline{D}(\mathbf{G}_p)$ is equal to $2 - \sqrt{2}$ for any value of p, as shown in Fig. 4. However, when the permutation $\varphi_b = (0, 1, 6, 7, 4, 5, 2, 3)$ is considered, the distance $d(\mathbf{G}_{0}^{2}, \mathbf{G}_{1}^{2})^{2}$ is given as $d(\mathbf{G}_{0}^{2}, \mathbf{G}_{1}^{2})^{2} = (C(0) - C(0))^{2}$ $C(1))^2 + (C(1) - C(6))^2 = 4$. An exhaustive enumeration of all couples gives $\overline{D}(\mathbf{G}^2) = 2$ (see (6)). The values of $\overline{D}(\mathbf{G}^p)$ are given for any truncation length p in Fig. 4. It can be seen that the proposed permutation significantly outperforms the identity permutation in terms of NMSD for all values of p > 1.

C. Optimization with simulated annealing and rotation symmetry

The number of possible length-q circular permutations φ of I_d is equal to (q-1)!. It prevents a brute-force search for q > 16 (e.g., 1.98×10^{87} for q = 64). Furthermore, finding the best permutation for p = 2 does not ensure the best permutation for p = 3 or p = q/4 for example. One can note the 4-fold rotational symmetry of the sequence obtained with 8-PSK.



Fig. 5. Optimized sequence for 64-PSK and 64-QAM.

This rotational symmetry reduces drastically the optimization problem's complexity.

It was deduced that optimization at p = q/4 leads to optimization at q/2, 3q/4, and q. The use of simulated annealing, combined with a constrained shape, and optimization at p = q/4 allowed us to find optimal solutions at p = q/4for 32-PSK and finally for 64-PSK modulation, as shown in Fig. 5 a) and Fig. 2. Besides, nearly optimal sequences were found for 64-QAM sequences using multi-objective simulated annealing as shown in Fig. 5 b) and Fig. 2 with objectives at p = 2, 3, 4, 5, 32, and 64. However, it does not allow finding a solution for 256-ary constellations.

D. Construction of a rate adaptive four cusps sequence using String art patterns

Someone familiar with string art can recognize in Fig. 5 a) a string art pattern. String art is a technique used by artists for the creation of abstract images, which are composed of straight lines of strings tensioned between pins distributed on a circular frame. A usual string art pattern is the cardioid shape which can also be seen in Fig. 5 a). The construction of a cardioid and *n*-cusped epicycloid is described in [9] (a cusp is a pointed end or part where two curves meet). The construction process described in [9] is modified such that one wire passes on each pin once only to give the same figure as in Fig. 5 a). The epicycloid sequence is defined by the recursion starting with $\varphi(0) = 0$ and followed by

$$\varphi(i+1) \equiv \varphi(i) \times (c+1) + a \mod q, \tag{8}$$

where $a \in -1, +1$ and c is the number of cusps. Using one cusp gives optimal distance only for p = q, two cusps give optimal distance for p = q and p = q/2, and four cusps for p = q, 3q/4, q/2 and q/4. In [9] is provided another process to construct a *n*-cusps hypocycloid called astroid when c =4. After modification, the astroid sequence is defined by the recursion starting with $\varphi(0) = 0$ and followed by

$$\varphi(i+1) \equiv -\varphi(i) \times (c-1) + a \mod q. \tag{9}$$

Fig. 6 shows the results for a 4-cusp epicycloid with q = 256 and an astroid with q = 64. In Fig. 6 b), the lines are extended to meet outside the circle to show the astroid shape.

Another type of sequence with the same properties, inspired by ZC sequences, can be constructed using the following recursion

$$\varphi(i+1) \equiv \varphi(i) + i \times c + a \mod q. \tag{10}$$



Fig. 6. 4-cusps epicycloid and astroid sequences

The sequences (8), (9) and (10) give six distinct ways of constructing sequences mapped onto high-order constellations that would be difficult to find using a brute-force search.

E. Construction of length q sequence mapped on a q/a-PSK constellation

From an astroid or epicycloid sequence of size q with permutation φ , it is possible to construct a new sequence with permutation φ' that allows a mapping on a constellation of size q/a with

$$\varphi'(i) = \left\lfloor \frac{\varphi}{a} \right\rfloor. \tag{11}$$

With q = 64, and a = 2, 4, or with q = 256, and a = 2, 4, 8, the obtained sequences maintain the same properties.

IV. 4-CUSPS RATE-ADAPTIVE SEQUENCE PROPERTIES

A. Square distance property

The codewords built from a 4-cusps sequence are either orthogonal or antipodal and have the same properties as biorthogonal codes giving

$$d(\mathbf{G}_i, \mathbf{G}_j)^2 = \begin{cases} 0, & \text{for } i = j. \\ 4, & \text{for } i \neq j, |i - j| = q/2. \\ 2, & \text{for } i \neq j, |i - j| \neq q/2. \end{cases}$$
(12)

Furthermore, the same remarkable property of bi-orthogonal codes is kept for punctured codewords of size p = q/4, q/2, and 3q/4. Another remarkable property is that codewords from epicycloid sequences with parameter a = 1 are orthogonal to codewords from epicycloid, astroid, and ZC-based sequences with parameter a = -1.

B. Per-symbol truncation

A fine-grained rate-adaptive decoder can be obtained by considering per symbol truncation as in [6]. This technique applies a different p value as a function of the jth symbol of an NB outer codeword.

When kq/4 , <math>k = 1, 2, 3 then $\overline{D} < 2$. However, it is possible to use per-symbol truncation with a proportion of kq/4 and (k+1)q/4 sequence giving an average length p for the symbols of the NB outer code. Consequently, we obtain $\overline{D} = 2$ for all symbols. Let us consider Fig. 4 with symbols mapped on 8-PSK CCSK sequences truncated to p = 7 giving $\overline{D} = 1.8$. Considering per-symbol truncation with the half first symbols with p = 8 and the other half with



Fig. 7. FER of 64-QAM and 64-PSK TCCSK

p = 6, the obtained symbols are with $\overline{D} = 2$ and an average length of p = 7.

Also, per-symbol truncation can be combined advantageously with a systematic NB code. The FER performances can be improved by giving more length to sequences associated with information symbols than sequences associated with redundant symbols.

C. Simulation Results

For all simulations, the NB decoder is an NB-LDPC decoder on GF(64) or GF(256) with the Extended Min-Sum algorithm [10], a Forward-Backward Check node implementation [11], and a maximum of 30 iterations. The Log-Likelihood Ratio of a symbol is computed as in [12]. We consider the complex Additive White Gaussian Noise (AWGN) channel, where the AWGN is of variance σ^2 , and the Signal-to-Noise Ratio (SNR) is defined as $1/\sigma^2$.

D. FER simulation results

Fig. 7 shows simulation results using PSK and QAM sequences of size q = 64. The PSK sequence is an epicycloid sequence. The QAM sequence is optimized for p = 2 and p = q/4. The simulations are performed using a $r_o = 1/3$ NB-LDPC code with k = 20 symbol (120 bits of information), and NB-LDPC decoder with $n_m = 20$ and $n_{op} = 25$. Simulation results of 5G are also shown for comparison. 5G simulation results are obtained using the LDPC Base Graph 1, 120 bits of information, layered offset min-sum decoding algorithm, and 30 iterations. With p = 1, results are equivalent to comparing the NB and binary code mapped on high-order modulation. The non-binary code performs better than the binary code due to the excellent behavior of the NB-LDPC code, mainly for high-order modulations and short frames. For NB code, the QAM mapping outperforms the PSK mapping because of its better minimum distance when p = 1, as shown in Fig. 2.

With p = 2, using (1), we get $s_e = \frac{1}{3} \times \frac{6}{2} = 1$. To get the same s_e with 5G, the 5G code rate is $r_c = 1/2$ and m = 2 bits for QPSK modulation, giving $s_e = m \times r_c = 1$. Similarly,



Fig. 8. Spectral efficiency of NB-CCSK(64) with 64-QAM modulation

p = 3 can be compared with $r_c = 1/3$ binary LDPC code and p = 5 can be compared with $r_c = 1/5$ binary LDPC code. Using per-symbol puncturing, p = 1.5 is achieved and can be compared with binary LDPC code with $r_c = 2/3$.

E. Spectral efficiency

To better illustrate the capacity range of NB-TCCSK, the spectral efficiency as a function of SNR is presented in Fig. 8. The numbers shown in the figure correspond to the p value. For a given efficiency s_e , the SNR at FER= 10^{-3} is reported. As a reference, we provide the maximal achievable coding rate using Shannon's noisy channel coding theorem [13] defined as $R = \log_2(1 + \text{SNR})$. Some 5G simulation results with LDPC base graph 1 and 120 information bits are also shown for comparison.

Fig. 9 shows simulation results using NB-CCSK of size q = 256 chips mapped on 256-QAM modulation. The NB-LDPC decoder is on GF(256), $r_o = 2/3$, $n_m = 70$, $n_{op} = 80$, $it_{max} = 30$ and the encoded information are of size k = 24 symbols (192 bits). The NB-CCSK performs better than the simulation results of 5G with LDPC base graph 1 and 192 information bits. For better visualization, low SNR performances are not presented. At low SNR, with p = 256, $s_e = \frac{2}{3} \times \frac{8}{256} = \frac{1}{48}$, the obtained SNR is -15.5 dB while Shannon limit is at -18.3 dB.

ACKNOWLEDGEMENT

This work has been funded by the French ANR under grants ANR-19-CE25-0013-01 (https://qcsp.univ-ubs.fr/) and ANR-21-CE25-0006 (https://ai4code.projects.labsticc.fr/).

V. CONCLUSION

This paper shows that a low SNR fine-grained rate-adaptive NB decoder can be obtained by combining an NB decoder with a truncated NB-CCSK modulation. The extension of binary sequence to NB sequence allows targeting higher SNRs. The paper presents new sequences mapped on q-ary constellation



Fig. 9. Spectral efficiency of NB-CCSK(256) with 256-APSK modulation

with optimal minimum distance at different levels of puncturing. The obtained rate range is impressive and allows targeting very low SNR.

REFERENCES

- M. Davey and D. Mackay, "Low density parity check codes over GF(q)," in 1998 Information Theory Workshop (Cat. No.98EX131), 1998, pp. 70–71.
- [2] G. Caire, G. Taricco, and E. Biglieri, "Bit-interleaved coded modulation," *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 927–946, 1998.
- [3] BeiDou Navigation Satellite System, Signal In Space, Interface Control Document, Open Service Signals B1C, China Satellite Navigation Office, 2017.
- [4] G. Dillard, M. Reuter, J. Zeiddler, and B. Zeidler, "Cyclic code shift keying: a low probability of intercept communication technique," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 39, no. 3, pp. 786–798, 2003.
- [5] Quasi-Zenith Satellite System Interface Specification Centimeter Level Augmented Service, Cabinet Office, IS-QZSS-L6-004, 2018.
- [6] C. Marchand and E. Boutillon, "Rate-adaptive inner code for non-binary decoders," in 2021 11th International Symposium on Topics in Coding (ISTC), 2021, pp. 1–5.
- [7] D. Chu, "Polyphase codes with good periodic correlation properties (corresp.)," *IEEE Transactions on Information Theory*, vol. 18, no. 4, pp. 531–532, 1972.
- [8] R. Frank, S. Zadoff, and R. Heimiller, "Phase shift pulse codes with good periodic correlation properties (corresp.)," *IRE Transactions on Information Theory*, vol. 8, no. 6, pp. 381–382, 1962.
- [9] J. S. Madachy, *mathematics on vacation*. Charles Scribner's Sons, 1966.
- [10] A. Voicila, D. Declercq, F. Verdier, M. Fossorier, and P. Urard, "Lowcomplexity decoding for non-binary LDPC codes in high order fields," *IEEE Transactions on Communications*, vol. 58, no. 5, pp. 1365–1375, 2010.
- [11] E. Boutillon and L. Conde-Canencia, "Bubble check: a simplified algorithm for elementary check node processing in extended min-sum non-binary LDPC decoders," *Electronics Letters*, vol. 46, no. 9, pp. pp– 633, 2010.
- [12] O. Abassi, L. Conde-Canencia, M. Mansour, and E. Boutillon, "Nonbinary coded CCSK and frequency-domain equalization with simplified LLR generation," in 2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2013, pp. 1478–1483.
- [13] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.