

SISO Decoding of \mathbb{Z}_4 Linear Kerdock and Preparata Codes

Aleksandar Minja, *Member, IEEE*, and Vojin Šenk, *Member, IEEE*

Abstract—Some nonlinear codes, such as Kerdock and Preparata codes, can be represented as binary images under the Gray map of linear codes over rings. This paper introduces MAP decoding of Kerdock and Preparata codes by working with their quaternary representation (linear codes over \mathbb{Z}_4) with the complexity of $O(N^2 \log_2 N)$, where N is the code length in \mathbb{Z}_4 . A sub-optimal bitwise APP decoder with good error-correcting performance and complexity of $O(N \log_2 N)$ that is constructed using the decoder lifting technique is also introduced. This APP decoder extends upon the original lifting decoder by working with likelihoods instead of hard decisions and is not limited to Kerdock and Preparata code families. Simulations show that our novel decoders significantly outperform several popular decoders in terms of error rate.

Index Terms—Codes over rings, Kerdock codes, MAP decoding, Preparata codes, Quaternary cyclic codes.

I. INTRODUCTION

Context and motivation. It was shown in [1] that some families of nonlinear binary codes with good properties can be represented as the binary image under the Gray map of linear codes over \mathbb{Z}_4 (the ring of integers modulo 4). These families include the Kerdock [2], Preparata [3], Goethals [4, 5] and Delsarte-Goethals [6] codes. It is well known that the quaternary Nordstrom-Robinson code [7] (also known as the “octacode” [8], which is used when the Leech lattice is constructed from eight copies of the face-centered cubic lattice [1]) is a self-dual code of length 8 and represents the initial member of both Kerdock and Preparata families [1].

The decoding of the nonlinear binary codes (and their \mathbb{Z}_4 linear counterparts) was an important area of research for years, and many hard and soft decision decoding algorithms were proposed. Almost all soft-decision decoding algorithms are based on an exhaustive search approach with respect to the Euclidean distance or the correlation between the received channel sequence and the possible transmitted codeword. With the exception of the Nordstrom-Robinson, there is no

low-complexity soft-input soft-output (SISO) decoder for the mentioned families of nonlinear binary codes. We believe this to be an important obstacle for their adoption in modern coding systems.

The primary purpose of this paper is to fill the void and provide the necessary tools for using these codes in modern coding systems. In this paper, we focus only on Kerdock and Preparata families, but similar techniques as the ones considered here can be used to design decoding algorithms for other related families.

Use of nonlinear codes and codes over rings in communication systems. There is widespread use of the Nordstrom-Robinson code in digital systems [9, 10]. A turbo product coding scheme with Nordstrom-Robinson as a component code was presented in [11, 12]. Kerdock codes for limited feedback MIMO systems were presented in [13, 14]. Space-time codes for standard phase shift keying (PSK) and quadrature amplitude modulation (QAM) signal constellations based on Kerdock and Delsarte-Goethals codes were presented in [15]. Quaternary constant-amplitude codes (codes that reduce the peak-to-average power ratio) for OFDM and MC-CDMA were presented in [16, 17]. Kerdock coded MC-CDMA system with non-linear amplifiers was presented in [18]. More recently, nonlinear codes are often used as components of product codes in order to achieve better reliability and security [19, 20]. Codes over rings have also found application in coding for the phase noise channel [21] and network-coded bidirectional relaying systems [22].

Brief overview of existing decoding algorithms. Common approaches for designing decoders for codes over rings include [23] the algebraic (syndrome) decoding of linear codes [24], the lifting decoder technique [25, 26], the partitioning of a code into the subcode and its cosets (a.k.a. the coset decomposition approach), introduced by Conway and Sloane in [27] (which works for both linear and nonlinear codes), and the permutation decoding [23, 28, 29]. Most of the soft decision decoders employ some form of the coset decomposition approach. E.g., for the Reed-Muller (RM) [2] subcode, we can use the fast Hadamard transform (FHT), which can significantly reduce the complexity of the decoder. A low complexity maximum likelihood (ML) decoding of Nordstrom-Robinson code was presented in [30]. An efficient implementation of this algorithm was presented in [31] and an improvement was proposed in [32]. A similar decoding algorithm of the same order of complexity was presented for Kerdock codes in [1] and [33]. A product code representation

This work was in part supported by the European Union Horizon 2020 research and innovation program under the WIDESPREAD grant agreement No 856967 and the Serbian Ministry of Education, Science and Technological Development through the project no. 451-03-68/2020-14/200156: "Innovative scientific and artistic research from the Faculty of Technical Sciences activity domain".

A. Minja is with the University of Novi Sad, Faculty of Engineering (Technical Sciences), Department of Power, Electronic and Telecommunication Engineering, Novi Sad 21000 Serbia e-mail: aminja@uns.ac.rs.

V. Šenk is with the University of Novi Sad, Faculty of Engineering (Technical Sciences), Department of Power, Electronic and Telecommunication Engineering, Novi Sad 21000 Serbia e-mail: vojcin_senk@uns.ac.rs.

Manuscript received March 20, 2021.

of nonlinear codes, using a high-complexity list-based ML decoding, along with a low-complexity bounded distance decoding algorithm based on coset decomposition, was presented in [19]. It was noted in [19] that effective decoding of Kerdock codes based on the proposed representation is left as an open problem. The standard way of implementing the maximum a posteriori (MAP) decoding of a linear code is via the Bahl–Cocke–Jelinek–Raviv (BCJR) algorithm [34], which uses a trellis representation of the code. The trellis complexity of Kerdock and Delsarte-Goethals codes was presented in [35], where a trellis representation consisting of parallel sections, each corresponding to a different coset of the $\text{RM}(1, m)$ ¹ subcode was considered. As the complexity of the BCJR algorithm for the $\text{RM}(1, m)$ code is $O(N^2)$ (where N is the length of the code) [36], the complexity of the BCJR decoding of the corresponding Kerdock code operating on this trellis would be $O(N^3)^2$. The trellis complexity of the Preparata and Goethals codes was investigated in [37]. A twisted squaring trellis construction based on the extended primitive double error correcting BCH code and its cosets was proposed in [37]. This construction is an extension of the Nordstrom-Robinson representation presented in [38]. A trellis representation of the Nordstrom-Robinson code based on the generalized array code was presented in [39]. A decoding algorithm based on this representation was investigated in [40]. Since trellis based decoding of Nordstrom-Robinson code is too complex, a new SISO decoding was proposed [9, 10]. The lifting decoder technique for decoding of free linear codes over rings was introduced in [25] and extended to arbitrary linear codes over rings in [26]. Chase decoding of linear \mathbb{Z}_4 codes based on the lifting decoder technique was presented in [41, 42]. Two algorithms for decoding of RM-like codes over rings of characteristic 2, based on coset decomposition were proposed in [16]. Though these algorithms primarily use hard-decision decoding, there is an extension to the soft-input case as well. Sphere decoding of Kerdock and Delsarte-Goethals codes was presented in [15]. Several algebraic decoders of codes over rings were presented in [1, 43, 44, 45, 46].

Contribution. In this paper, we present symbol-wise MAP decoding algorithms for Kerdock and Preparata codes with complexity $O(N^2 \log_2 N)$ (where N is the code length in \mathbb{Z}_4). This is the same order of complexity as the ML decoding algorithms of Kerdock codes, presented in [1, 30, 33]. To the best of our knowledge, no MAP decoding algorithms were presented for these codes. We further present a sub-optimal bitwise APP decoding algorithm based on the lifting decoder technique [25] that performs within 1.5dB of the optimum and has the complexity of $O(N \log_2 N)$. This sub-optimal decoder can be applied to any linear \mathbb{Z}_4 code, but the decoding complexity depends on the encoder and decoder complexity of its associated binary code. Although there are several soft input decoders, these are the first probabilistic SISO decoders for these code families (with the exception of

the BCJR decoder, whose complexity was noted to be too high, and the Nordstrom-Robinson code) that we know of. We note that a low-complexity bit-wise SISO decoder for the Nordstrom-Robinson code, based on the binary nonlinear representation, was investigated in [9, 10]. As the quaternary Nordstrom-Robinson code belongs to both the Kerdock and the Preparata families, it can efficiently be decoded using any of the novel MAP decoders or the lifting decoder presented in this paper. This is demonstrated in Section V. The novel decoding algorithms are compared to the original lifting decoder [25] and the chase decoder [41, 42], and it is shown that our decoders significantly outperform these algorithms for the case of both Kerdock and Preparata codes.

Paper organization. The remainder of this paper is composed of five sections. Section II introduces the necessary definitions and presents the system model analyzed in this paper. Section III introduces MAP decoding of Kerdock and Preparata codes. Section IV presents a fast, sub-optimal, soft input, soft output decoding algorithm for Kerdock and Preparata codes. Section V presents simulation results, and Section VI concludes the paper.

Notation. Throughout this paper, bold letters are used to represent module elements³ and the standard function notation is used to represent polynomials. The i -th component (term) of an element \mathbf{x} (polynomial $x(Z)$, where Z is a dummy variable), is denoted x_i . Given two elements, \mathbf{x} and \mathbf{y} of length N , $\mathbf{x} \odot \mathbf{y} = [x_0 y_0, x_1 y_1, \dots, x_{N-1} y_{N-1}]$ represents the Hadamard (point-wise) product, and $\langle \mathbf{x}; \mathbf{y} \rangle$ represents the scalar product. Upper case letters represent matrices, where \mathbf{x}_n denotes the n -th row of some matrix X . $P[x]$ represents the probability of x and $P[x|y]$ represents the conditional probability of x given y . For convenience, $\delta_{a,b}$ represents the Kronecker delta, defined as $\delta_{a,b} = 1$ if $a = b$ and $\delta_{a,b} = 0$ if $a \neq b$. Standard blackboard bold letters are used for sets of numbers (and the corresponding rings/fields over them), i.e. \mathbb{Z} is the set of integers, \mathbb{R} is the set of real numbers and \mathbb{C} is the set of complex numbers. $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ represents the set of integers modulo n . \mathbb{K}^N represents the set of all N -tuples of a set \mathbb{K} . Cursive uppercase letters represent codes and other sets. Other notation is introduced as it is used.

II. SYSTEM MODEL

Let operators $+$ and \cdot represent addition and multiplication in \mathbb{Z}_4 , while \oplus and \otimes represent addition and multiplication in \mathbb{Z}_2 . Note that $\mathbb{Z}_2 \subset \mathbb{Z}_4$, so the elements $\{0, 1\} \in \mathbb{Z}_2$ can be regarded as the same elements in \mathbb{Z}_4 . Furthermore, any element $\alpha \in \mathbb{Z}_4$ has a dyadic expansion (representation)

$$\alpha = a + 2 \cdot b, \text{ with } a, b \in \mathbb{Z}_2. \quad (1)$$

We will often write the dyadic expansion of α as a tuple (a, b) , where identity $2a = 2\alpha$ follows from (1). The dyadic expansion can naturally be extended to module elements and matrices over \mathbb{Z}_4 . For completeness, we reproduce the *Lemma 1* from [25] for the case of $\mathbb{Z}_4 = \mathbb{Z}_2^2$, [25, Lemma 1]: Let m, n

¹Where $\text{RM}(r, m)$ represents the r -order RM code of length 2^m [24].

²It was noted in [35] that the Viterbi decoding on the biproper trellis would improve run-time performance by up to 10%, compared with the decoding on the trellis consisting of parallel cosets of the $\text{RM}(1, m)$ code.

³As every vector space is by definition a free module, we will also refer to vector spaces as modules and to vectors as elements.

be natural numbers and let $\mathbf{v} \in \mathbb{Z}_2^m$, $\mathbf{w} \in \mathbb{Z}_2^n$ and $G \in \mathbb{Z}_2^{m \times n}$. Then

$$2 \cdot (\mathbf{v} \otimes G \oplus \mathbf{w}) = 2 \cdot (\mathbf{v} \cdot G + \mathbf{w}).$$

This identity will be used later on.

An $[N, K = k_1 + k_2]$ linear code of type $4^{k_1} 2^{k_2}$ over \mathbb{Z}_4 is a submodule of \mathbb{Z}_4^N , defined by a generator matrix G . If $k_2 = 0$, the corresponding code is a free submodule and the generator matrix can be written in the systematic form - consisting of the identity and the parity part. Both Kerdock and Preparata codes can be regarded as free submodules of \mathbb{Z}_4^N [1].

A. Short Review of Kerdock and Preparata Codes

Nonlinear binary Kerdock code of length 2^m (for some even m , $m \geq 4$) is constructed as a union of the $\text{RM}(1, m)$ code and its cosets in the $\text{RM}(2, m)$ [24], i.e. every Kerdock code is a supercode of the $\text{RM}(1, m)$ code and a subcode of the $\text{RM}(2, m)$ code [2]. Similarly, the nonlinear binary Preparata code of length 2^m (for some even m , $m \geq 4$) can be constructed as a union of the $\text{RM}(m-3, m)$ code and its cosets in the $\text{RM}(m-2, m)$ [3, 24]. In the case of $m = 4$, we have the Nordstrom-Robinson code. It was shown in [1] that these nonlinear codes can be represented as the binary images under the Gray map of cyclic codes over the \mathbb{Z}_4 ring.

When considering cyclic codes over fields it is common to talk about extensions of base fields. A similar approach is used for rings [1]. We define a Galois ring as an extension of the base ring \mathbb{Z}_4 . Let $h(Z)$ be an irreducible monic polynomial of order m over \mathbb{Z}_4 (where Z is the dummy variable), then the Galois ring GR is isomorphic to the set of all polynomials modulo $h(Z)$, $\mathbb{Z}_4[Z]/h(Z)$. Every GR has a primitive element ξ of order $N-1$, where $N = 2^m$. It is clear that ξ does not generate the entire ring, but every element $\alpha \in GR$ has a dyadic representation [1]

$$\alpha = \xi^r + 2\xi^s, \quad r, s \in \Delta = \{-\infty, 0, 1, \dots, N-2\}, \quad (2)$$

with a standard convention, $\xi^{-\infty} = 0$, and $\xi^{-\infty} \xi^r = 0$, $\forall r \in \Delta$.

The generator matrix of the extended Kerdock code $\mathcal{K}[2^m, m+1]$, is defined as [1],

$$G_{\mathcal{K}} = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \xi & \xi^2 & \cdots & \xi^{N-2} \end{bmatrix} P_{\pi}, \quad (3)$$

where P_{π} is an $N \times N$ column permutation matrix. Let $(G_{\mathcal{K},0}, G_{\mathcal{K},1})$ represent the dyadic expansion of the generator matrix $G_{\mathcal{K}}$. The binary linear code defined by the generator matrix $G_{\mathcal{K},0}$ is called the associated binary code [47]. Matrix $G_{\mathcal{K},0}$ can be obtained from $G_{\mathcal{K}}$ by replacing ξ^n , $n \in \Delta$ with $\bar{\xi}^n$, $n \in \Delta$, where $\bar{\xi}$ is a primitive element of the irreducible monic polynomial $\bar{h}(Z) \in \mathbb{Z}_2[Z]$, chosen so that $\bar{h}(Z) \equiv h(Z) \pmod{2}$ [1, 47]. Since $\bar{\xi}$ is a primitive root of order $N-1$, the set $\{\bar{\xi}^n \mid n \in \Delta\}$ corresponds to the set of all m -dimensional module elements over \mathbb{Z}_2 , which implies that $G_{\mathcal{K},0}$ is in fact the generator matrix of the $\text{RM}(1, m)$ code. For a detailed proof see [47, Corollary 8.4]. Column permutation matrix P_{π} is chosen so that the associated binary code of the Kerdock code is the first order Reed-Muller code $\text{RM}(1, m)$ obtained from a Sylvester-type binary Hadamard

matrix [24]. This makes it possible to apply the fast Walsh-Hadamard transform, and significantly reduce the complexity of the decoding algorithm.

The extended Preparata code $\mathcal{P}[2^m, 2^m - m - 1]$, is the dual of the extended Kerdock code, defined by the parity check matrix $H_{\mathcal{P}} = G_{\mathcal{K}}$. We assume that the generator matrix $G_{\mathcal{P}}$ is given in a systematic form⁴ (this follows from the fact that $G_{\mathcal{K}}$ can easily be reduced to a systematic form by only row operations). It can easily be verified that the associated binary code of the Preparata code is in fact the $\text{RM}(m-2, m)$ code [47, Corollary 9.3]. Note that the encoding complexity of both the Kerdock and Preparata code is $O(N \log_2 N)$. This is an important fact that will be used later on.

B. Communication System and MAP Decoding

Let C be an arbitrary $[N, K]$ linear block code over some ring \mathbb{K} , and let all the codewords be equally likely. Given a codeword $\mathbf{c} \in C$ and a modulation mapping $\phi(\cdot)$, the corresponding modulated codeword is $\mathbf{x} = \phi(\mathbf{c})$. The random mapping $\Omega(\cdot)$ represent a memoryless channel, defined by a conditional probability

$$P[\mathbf{y}|\mathbf{c}] = \prod_{n=0}^{N-1} P[y_n|c_n], \quad (4)$$

where $\mathbf{y} = \Omega(\mathbf{x})$ is a specific channel output. For every codeword symbol c_j , $j \in \{0, 1, \dots, N-1\}$, the goal of the MAP decoder is to find $P[c_j = \alpha|\mathbf{y}]$ for every $\alpha \in \mathbb{K}$ and choose the maximum one. Using Bayes's rule and the definition of the memoryless channel, we can write

$$\begin{aligned} P[c_j = \alpha|\mathbf{y}] &= \sum_{\mathbf{b} \in C} P[\mathbf{b}|\mathbf{y}] \delta_{b_j, \alpha} \\ &= \sum_{\mathbf{b} \in C} \frac{P[\mathbf{b}]}{P[\mathbf{y}]} P[\mathbf{y}|\mathbf{b}] \delta_{b_j, \alpha} \\ &= \frac{1}{|C|P[\mathbf{y}]} \sum_{\mathbf{b} \in C} \prod_{n=0}^{N-1} P[y_n|b_n] \delta_{b_j, \alpha}, \end{aligned} \quad (5)$$

where $|C|$ represents the size of the code C .

A MAP decoding rule for codes over finite fields using the dual code was introduced in [48] and extended to codes over rings in [49, 50]. Let the Fourier transform ($\mathcal{F}\{\cdot\}$) of a real or complex-valued function $f(\alpha)$, $\alpha \in \mathbb{K}$, be defined as

$$\mathcal{F}\{f(\alpha)\} = \sum_{\alpha \in \mathbb{K}} \omega^{-\alpha\beta} f(\alpha) = F(\beta), \quad \beta \in \mathbb{K}, \quad (6)$$

with

$$\omega = \exp\left\{\frac{2\pi I}{|\mathbb{K}|}\right\}, \quad I = \sqrt{-1}. \quad (7)$$

Using the Poisson summation formula and the fact that the Fourier transform of a product function is the product of the corresponding individual Fourier transforms [50, 51], the MAP decoding rule in (5), can be written as

$$P[c_j = \alpha|\mathbf{y}] = \frac{1}{|\mathbb{K}|^N P[\mathbf{y}]} \sum_{\mathbf{b} \in C^\perp} \prod_{n=0}^{N-1} \mathcal{F}\{P[y_n|b_n]\} \mathcal{F}\{\delta_{b_j, \alpha}\},$$

⁴By *systematic form*, we assume that a subset of columns of the generator matrix form the identity matrix, while the remaining columns represent parity.

where C^\perp is the dual code of C and $|\mathbb{K}|^N = |C| \cdot |C^\perp|$. By substituting eq. (6) for the Kronecker delta we get

$$\begin{aligned} P[c_j = \alpha | \mathbf{y}] &= \eta \sum_{\mathbf{b} \in C^\perp} \prod_{n=0}^{N-1} \mathcal{F}\{P[y_n | b_n]\} \sum_{\beta \in \mathbb{K}} \omega^{-\alpha\beta} \delta_{b_j, \beta} \\ &= \eta \sum_{\beta \in \mathbb{K}} \omega^{-\alpha\beta} \sum_{\mathbf{b} \in C^\perp} \prod_{n=0}^{N-1} \mathcal{F}\{P[y_n | b_n]\} \delta_{b_j, \beta}, \end{aligned} \quad (8)$$

where $\eta = \frac{1}{|\mathbb{K}|^N P[\mathbf{y}]}$. After substituting eq. (6) in (8) we have

$$P[c_j = \alpha | \mathbf{y}] = \eta \sum_{\beta \in \mathbb{K}} \omega^{-\alpha\beta} \sum_{\mathbf{b} \in C^\perp} \left[\prod_{n=0}^{N-1} \sum_{\gamma \in \mathbb{K}} \omega^{-\gamma b_n} P[y_n | \gamma] \cdot \delta_{b_j, \beta} \right]. \quad (9)$$

By using the identity $\delta_{a,b} = \frac{1}{|\mathbb{K}|} \sum_{\gamma \in \mathbb{K}} \omega^{\gamma \cdot (a-b)}$ and a little arithmetic, we get

$$P[c_j = \alpha | \mathbf{y}] = \frac{\eta}{|\mathbb{K}|} A_j(\alpha), \quad \alpha \in \mathbb{K} \quad (10)$$

where

$$A_j(\alpha) = \sum_{\beta \in \mathbb{K}} \omega^{-\alpha\beta} \sum_{\mathbf{b} \in C^\perp} \left[\prod_{n=0}^{N-1} \sum_{\gamma \in \mathbb{K}} \omega^{-\gamma(b_n - \beta \delta_{j,n})} P[y_n | \gamma] \right].$$

III. MAP DECODING ALGORITHM

Let $\mathbb{S} = \mathbb{R}[Z]/(Z^4 - 1)$, be a set of all polynomials over \mathbb{R} , modulo $Z^4 - 1$, where Z is a dummy variable. Note that the multiplicative group of monic monomials in \mathbb{S} is equivalent to the additive group of \mathbb{Z}_4 . For convenience, we define a mapping $\zeta : \mathbb{Z}_4 \rightarrow \mathbb{S}$, such that $\zeta(\alpha) = Z^\alpha$, where a natural extension to elements and matrices is to apply $\zeta(\cdot)$ componentwise. Given $f(Z) = \sum_{\alpha \in \mathbb{Z}_4} f_\alpha Z^\alpha \in \mathbb{S}$ and $Z^{-\beta} \in \mathbb{S}$, $\beta \in \mathbb{Z}_4$, then

$$f(Z) \cdot Z^{-\beta} = \sum_{\alpha \in \mathbb{Z}_4} f_\alpha Z^{\alpha-\beta} = \sum_{\alpha \in \mathbb{Z}_4} f_{\alpha+\beta} Z^\alpha \in \mathbb{S}. \quad (11)$$

Furthermore, let $C' \subseteq C$ be a linear $[N, K-1]$ subcode of C , such that $\mathbf{1} \notin C'$, where $\mathbf{1}$ is the all-one element of length N . We assume that all codewords $\mathbf{c} \in C'$ are enumerated, and arranged in a matrix A , such that the k -th row of A is equal to the k -th codeword \mathbf{c}_k . Similar to denotations in [36], let $D = \zeta(A)$ and $\bar{D} = \zeta(-A)$, be two $4^{K-1} \times N$ matrices.

We again assume a codeword $\mathbf{c} \in C$ is transmitted over a memoryless channel, and \mathbf{y} is received. Following the group algebra description of MAP decoding from [36], we first compute the reliability element $\mathbf{w} \in \mathbb{S}^N$, where each component is a log-likelihood polynomial, defined as

$$w_n(Z) = \sum_{\alpha \in \mathbb{Z}_4} \log P[y_n | \alpha] Z^\alpha, \quad n = 0, \dots, N-1. \quad (12)$$

We compute sums of logarithms of probabilities of receiving the channel output \mathbf{y} conditioned on the sent codeword, as

$$\mathbf{t}^\top = \bar{D} \mathbf{w}^\top \in \mathbb{S}^{4^{K-1}}, \quad (13)$$

where we use *Proposition 2* from [36], which we summarize here, [36, **Proposition 2**]: Given a reliability element \mathbf{w} and

a codeword $\mathbf{c}_k \in C$ the following identity holds:

$$\begin{aligned} t_k(Z) &= \langle \mathbf{w}; \zeta(-\mathbf{c}_k) \rangle \\ &= \sum_{\alpha \in \mathbb{Z}_4} t_{k,\alpha} Z^\alpha = \sum_{\alpha \in \mathbb{Z}_4} \sum_{n=0}^{N-1} \log P[y_n | \alpha + c_{k,n}] Z^\alpha \\ &= \sum_{\alpha \in \mathbb{Z}_4} \log P[\mathbf{y} | \mathbf{c}_k + \alpha \mathbf{1}] Z^\alpha, \quad \mathbf{c}_k \in C. \end{aligned} \quad (14)$$

Next, we recompute the sums of logarithms of probabilities into products of probabilities, $\mathbf{v} \in \mathbb{S}^{4^{K-1}}$, as follows

$$v_k(Z) = \sum_{\alpha \in \mathbb{Z}_4} e^{t_{k,\alpha}} Z^\alpha, \quad k = 0, \dots, 4^{K-1} - 1. \quad (15)$$

Finally, we compute soft decisions $\mathbf{s}^\top = D^\top \mathbf{v}^\top \in \mathbb{S}^N$, where

$$s_n(Z) = \sum_{\alpha \in \mathbb{Z}_4} Z^\alpha \sum_{\mathbf{b} \in C} P[\mathbf{y} | \mathbf{b}] \delta_{b_j, \alpha}, \quad n = 0, \dots, N-1. \quad (16)$$

The MAP decision is by definition, $c_n = \beta$, such that $s_{n,\beta} = \max_{\alpha \in \mathbb{Z}_4} \{s_{n,\alpha}\}$ (i.e. β is the index of the largest real-valued term in the polynomial $s_n(Z) \in \mathbb{S}$), for all $n = 0, \dots, N-1$. It is clear that the most computationally expensive steps are multiplications with D and \bar{D} . In the following subsection, we will show how this can be simplified in the case of the Kerdock code. In the case of the Preparata code, we will use the dual MAP decoding rule, given in (10).

Consider the codeword $\mathbf{c} = \mathbf{u} \cdot G \in \mathbb{Z}_4^N$, where $G \in \mathbb{Z}_4^{K \times N}$ is the generator matrix and $\mathbf{u} \in \mathbb{Z}_4^K$ is the corresponding information sequence. Let $(\mathbf{u}_0, \mathbf{u}_1)$ and (G_0, G_1) represent the dyadic expansions of the information sequence and the generator matrix, respectively. From the dyadic expansion of the information sequence, it follows that

$$\mathbf{c} = \mathbf{u} \cdot G = (\mathbf{u}_0 + 2 \cdot \mathbf{u}_1) \cdot G = \mathbf{u}_0 \cdot G + 2 \cdot (\mathbf{u}_1 \otimes G_0), \quad (17)$$

where the last equality follows from *Lemma 1* in [25]. It is well known that in the case of the Kerdock and Preparata codes, the G_0 is the generator matrix of the corresponding RM subcode [1].

A. MAP Decoding of Kerdock codes

Let G be the Kerdock generator matrix, defined in (3). We will define three auxiliary matrices, $A_0 \in \mathbb{Z}_4^{4 \times N}$, $A_1 \in \mathbb{Z}_2^{N \times N}$ and $A_2 \in \mathbb{Z}_2^{N \times N}$, together with their row sets (sets of row elements), \mathcal{A}_0 , \mathcal{A}_1 and \mathcal{A}_2 . Let the rows of A_0 be $\alpha \mathbf{1}$, $\alpha \in \mathbb{Z}_4$. Let the rows of A_1 be equal to $\mathbf{i} \cdot G$, where $\mathbf{i} \in \mathbb{Z}_2^K$ is a binary sequence of length K , such that the first value is always zero. Finally, let the rows of A_2 be equal to $2 \cdot (\mathbf{i} \otimes G_0)$, where \mathbf{i} is the same as in the previous case. Note that $A_2 = 2 \cdot A_1 = 2 \cdot H_{2^m}$, where H_{2^m} is the binary Hadamard matrix, which follows from the fact that the associated binary code of the Kerdock code is the RM(1, m) code. We can now define the Kerdock code as

$$\mathcal{K} = \{\mathbf{a}^0 + \mathbf{a}^1 + \mathbf{a}^2 | \mathbf{a}^0 \in \mathcal{A}_0, \mathbf{a}^1 \in \mathcal{A}_1, \mathbf{a}^2 \in \mathcal{A}_2\}, \quad (18)$$

while the linear subcode $\mathcal{K}' \subseteq \mathcal{K}$, that does not contain the all-one codeword, can be represented as

$$\mathcal{K}' = \{\mathbf{a}^1 + \mathbf{a}^2 | \mathbf{a}^1 \in \mathcal{A}_1, \mathbf{a}^2 \in \mathcal{A}_2\}. \quad (19)$$

Algorithm 1 In-place Fast Walsh-Hadamard transform

Input: a ,
Output: a ,
 1: **for** $h = 1; h < N; h \leftarrow 2 \cdot h$ **do**
 2: **for** $i = 0; i < N; i \leftarrow i + 2 \cdot h$ **do**
 3: **for** $j = i$ **to** $i + h$ **do**
 4: $x \leftarrow a_j, y \leftarrow a_{j+h}$, {Save current values}
 5: $a_j \leftarrow x + y$, {Calculate new a_j value}
 6: $a_{j+h} \leftarrow x + Z^2 \cdot y$, {Calculate new a_{j+h} value}
 7: **end for**
 8: **end for**
 9: **end for**

Note that this representation is equivalent to the trace representation of the Kerdock code, introduced in [1]. Let $D_1 = \underline{\zeta}(A_1)$ and $D_2 = \underline{\zeta}(A_2)$. Similarly, let $\bar{D}_1 = \underline{\zeta}(-A_1)$ and $\bar{D}_2 = \underline{\zeta}(-A_2) = D_2$. As any row of A can be represented as a sum of rows from A_1 and A_2 , it follows that any row $\mathbf{d}_k = \underline{\zeta}(\mathbf{c}_k)$ of D can be represented as $\mathbf{d}_n^1 \odot \mathbf{d}_l^2$, where \mathbf{d}_n^1 is a row from D_1 and \mathbf{d}_l^2 is a row from D_2 .

Given the channel output \mathbf{y} , we again start the decoding process by computing $\mathbf{w} \in \mathbb{S}^N$ using eq. (12). We note that

$$t_k(Z) = \langle \mathbf{w}; \bar{\mathbf{d}}_n^1 \odot \mathbf{d}_l^2 \rangle = \langle \mathbf{w} \odot \bar{\mathbf{d}}_n^1; \mathbf{d}_l^2 \rangle, \quad (20)$$

where the last equality follows from the commutativity of multiplication. Instead of applying eq. (13), we first define a matrix $B \in \mathbb{S}^{N \times N}$, with rows $\mathbf{b}_n = \mathbf{w} \odot \bar{\mathbf{d}}_n^1$, $n = 0, \dots, N-1$. Note that every component of B is equal to

$$b_{n,l}(Z) = \sum_{\alpha \in \mathbb{Z}_4} \log P[\mathbf{y}_l | a_{n,l}^1 + \alpha] Z^\alpha, \quad n, l = 0, \dots, N-1. \quad (21)$$

Next, we will compute the matrix of the sums of logarithms of probabilities

$$T = B \cdot D_2^T. \quad (22)$$

This multiplication can be efficiently implemented by applying a modified fast Walsh-Hadamard transform (FWHT), presented in Algorithm 1, to every row of B , $\mathbf{t}_n = \text{FWHT}(\mathbf{b}_n)$, $n = 0, \dots, N-1$. Note that every component of T is equal to

$$t_{n,l}(Z) = \sum_{\alpha \in \mathbb{Z}_4} Z^\alpha \sum_{j=0}^{N-1} \log P[\mathbf{y}_l | a_{n,j}^1 + a_{l,j}^2 + \alpha], \quad (23)$$

$$n, l = 0, \dots, N-1.$$

Let $V \in \mathbb{S}^{N \times N}$ be a matrix of products of probabilities, with components

$$\begin{aligned} v_{n,l}(Z) &= \sum_{\alpha \in \mathbb{Z}_4} Z^\alpha \exp \{t_{n,l,\alpha}\} \\ &= \sum_{\alpha \in \mathbb{Z}_4} Z^\alpha \prod_{j=0}^{N-1} P[\mathbf{y}_l | a_{n,j}^1 + a_{l,j}^2 + \alpha] \\ &= \sum_{\alpha \in \mathbb{Z}_4} P[\mathbf{y}_l | \mathbf{c}_k + \alpha \mathbf{1}] Z^\alpha, \end{aligned} \quad (24)$$

where $\mathbf{c}_k = \mathbf{a}_n^1 + \mathbf{a}_l^2$ and $n, l = 0, \dots, N-1$.

Algorithm 2 MAP decoding of Kerdock codes

Input: \mathbf{y} ,
Output: \mathbf{s}
 1: Compute the reliability element \mathbf{w} using eq. (12).
 2: **for** $n = 0; n < N; n \leftarrow n + 1$ **do**
 3: $\mathbf{t}_n \leftarrow \text{FWHT}(\mathbf{w} \odot \bar{\mathbf{d}}_n^1)$,
 4: **end for**
 5: **for** $n = 0; n < N; n \leftarrow n + 1$ **do**
 6: {Compute element $\mathbf{v}_n \in \mathbb{S}^N$ as follows}
 7: **for** $l = 0; l < N; l \leftarrow l + 1$ **do**
 8: $v_{n,l}(Z) \leftarrow \sum_{\alpha \in \mathbb{Z}_4} Z^\alpha \exp \{t_{n,l,\alpha}\}$
 9: **end for**
 10: **end for**
 11: $\mathbf{s} \leftarrow \mathbf{0}$ {Initialize \mathbf{s} to the all-zero value}
 12: **for** $n = 0; n < N; n \leftarrow n + 1$ **do**
 13: $\mathbf{s} \leftarrow \mathbf{s} + \text{FWHT}(\mathbf{v}_n) \odot \mathbf{d}_n^1$,
 14: **end for**

Next, we compute $Q = V \cdot D_2 \in \mathbb{S}^{N \times N}$, with

$$\begin{aligned} q_{n,l}(Z) &= \sum_{j=0}^{N-1} Z^{a_{l,j}^2} \cdot v_{n,j} \\ &= \sum_{\alpha \in \mathbb{Z}_4} Z^\alpha \sum_{j=0}^{N-1} P[\mathbf{y} | \mathbf{c}_k + (\alpha - a_{l,j}^2) \mathbf{1}], \end{aligned} \quad (25)$$

where $\mathbf{c}_k = \mathbf{a}_n^1 + \mathbf{a}_j^2$, and $n, l = 0, \dots, N-1$. This product can also be efficiently implemented by applying FWHT transforms to every row of V . Finally, let the element of soft decisions $\mathbf{s} \in \mathbb{S}^N$ be equal to

$$\mathbf{s} = \sum_{j=0}^{N-1} \mathbf{d}_j^1 \odot \mathbf{q}_j, \quad (26)$$

with

$$\begin{aligned} s_n(Z) &= \sum_{i=0}^{N-1} Z^{a_{i,n}^2} \cdot q_{n,i} \\ &= \sum_{\alpha \in \mathbb{Z}_4} \sum_{j=0}^{N-1} \sum_{i=0}^{N-1} P[\mathbf{y} | \mathbf{c}_k + (\alpha - a_{i,j}^2 - a_{i,n}^2) \mathbf{1}] \\ &= \sum_{\alpha \in \mathbb{Z}_4} Z^\alpha \sum_{\mathbf{b} \in \mathcal{C}} P[\mathbf{y} | \mathbf{b}] \delta_{b_j, \alpha}, \quad n = 0, \dots, N-1. \end{aligned} \quad (27)$$

This concludes the algorithm. We summarize the MAP decoding of Kerdock codes in Algorithm 2.

Calculating \mathbf{s} and forming matrices B and V have complexity $O(N^2)$, while for computing the matrices T and Q , we have N uses of the FWHT transform, with complexity $O(N \log_2 N)$, so the total complexity of this decoding algorithm is $O(N^2 \log_2 N)$. A detailed complexity analysis of Algorithm 2 is given in Table I. All operations are assumed to be carried out over the polynomial ring \mathbb{S} . As polynomials in \mathbb{S} can efficiently be implemented as floating-point arrays of length 4, with multiplication implemented as circular convolution (with complexity $4^2 O(1)$) and addition implemented

TABLE I
THE COMPUTATIONAL COST OF MAP DECODING OF KERDOCK CODES

Steps	Short description	Complexity
1.	Compute \mathbf{w}	$\mathcal{O}(N)$
2. - 4.	FWHT of $\mathbf{w} \odot \bar{\mathbf{d}}_n$	$N\mathcal{O}(N \log_2 N) = \mathcal{O}(N^2 \log_2 N)$
5. - 10.	Calculate matrix V	$\mathcal{O}(N^2)$
11.	Initialize \mathbf{s}	$\mathcal{O}(N)$
12. - 14.	Compute \mathcal{Q} and \mathbf{s}	$N\mathcal{O}(N \log_2 N) = \mathcal{O}(N^2 \log_2 N)$

as component-wise addition (with complexity $4\mathcal{O}(1)$), the additional computational cost can be treated as a constant term.

B. MAP Decoding of Preparata codes

Consider a Preparata code with a parity-check matrix defined in eq. (3). Given the channel output \mathbf{y} , we begin the decoding process by calculating the element of likelihoods $\mathbf{w} \in \mathbb{S}^N$, with

$$w_n(Z) = \sum_{\alpha \in \mathbb{Z}_4} P[y_n|\alpha]Z^\alpha. \quad (28)$$

Next, we calculate the element \mathbf{r} as the componentwise Fourier transform of \mathbf{w} , with

$$r_n(Z) = \mathcal{F}(\mathbf{w}_n) = \sum_{\alpha \in \mathbb{Z}_4} Z^\alpha \sum_{\gamma \in \mathbb{Z}_4} \omega^{-\alpha\gamma} P[y_n|\gamma]. \quad (29)$$

Let functions $|\cdot|$ and $\arg\{\cdot\}$ represent the modulus and the argument of a complex number, respectively. We will form elements $\boldsymbol{\rho} \in \mathbb{S}^N$ and $\boldsymbol{\phi} \in \mathbb{S}^N$, with components

$$\rho_n(Z) = \sum_{\alpha \in \mathbb{Z}_4} \log|r_{n,\alpha}|Z^\alpha, \quad (30)$$

and

$$\phi_n(Z) = \sum_{\alpha \in \mathbb{Z}_4} \arg\{r_{n,\alpha}\}Z^\alpha. \quad (31)$$

Next, we compute elements $\mathbf{t} \in \mathbb{S}^{4^{K-1}}$ and $\mathbf{e} \in \mathbb{S}^{4^{K-1}}$ as

$$\mathbf{t}^T = \bar{D}\boldsymbol{\rho}^T, \quad (32)$$

and

$$\mathbf{e}^T = \bar{D}\boldsymbol{\phi}^T. \quad (33)$$

Note that similarly as in the case of the Kerdock code, we can efficiently calculate the element \mathbf{t} , by first computing the matrix $B \in \mathbb{S}^{N \times N}$ with rows $\mathbf{b}_n = \boldsymbol{\rho} \odot \bar{\mathbf{d}}_n$, $n = 0, \dots, N-1$, and then computing the matrix $T \in \mathbb{S}^{N \times N}$ with rows $\mathbf{t}_n = \text{FWHT}(\mathbf{b}_n)$, $n = 0, \dots, N-1$. Every component of \mathbf{t} now corresponds to one component of matrix T . We apply the same procedure to get the matrix $E \in \mathbb{S}^{N \times N}$ that corresponds to element \mathbf{e} .

Next, we form an $N \times N$ matrix V with components

$$v_{n,l}(Z) = \sum_{\alpha \in \mathbb{Z}_4} \exp\{t_{n,l,\alpha}\} \cdot \exp\{e_{n,l,\alpha}\}Z^\alpha. \quad (34)$$

Let \mathcal{Q} be an $N \times N$ matrix with rows $\mathbf{q}_n = \text{FWHT}(\mathbf{v}_n)$, $n = 0, \dots, N-1$. We calculate element \mathbf{s} as

$$\mathbf{s} = \sum_{n=0}^{N-1} \mathbf{d}_n^1 \odot \mathbf{q}_n, \quad (35)$$

TABLE II
THE COMPUTATIONAL COST OF MAP DECODING OF PREPARATA CODES

Steps	Short description	Complexity
1.	Compute \mathbf{w}	$\mathcal{O}(N)$
2.	Compute \mathbf{r}	$\mathcal{O}(N)$
3. - 6.	Compute $\boldsymbol{\rho}$ and $\boldsymbol{\phi}$	$\mathcal{O}(N)$
7. - 10.	Compute T and E	$N\mathcal{O}(N \log_2 N) = \mathcal{O}(N^2 \log_2 N)$
11. - 16.	Calculate matrix V	$\mathcal{O}(N^2)$
17.	Initialize \mathbf{s}	$\mathcal{O}(N)$
18. - 20.	Compute V and \mathbf{s}	$N\mathcal{O}(N \log_2 N) = \mathcal{O}(N^2 \log_2 N)$
21.	Compute \mathbf{g}	$\mathcal{O}(N)$
22.	Compute \mathbf{h}	$\mathcal{O}(N)$
23. - 25.	Compute \mathbf{z}	$\mathcal{O}(N)$

with

$$s_j(Z) = \sum_{\alpha \in \mathbb{Z}_4} Z^\alpha \sum_{\mathbf{b} \in \mathbb{C}^L} \delta_{b_j, \alpha} \prod_{n=0}^{N-1} \sum_{\gamma \in \mathbb{Z}_4} \omega^{-\gamma(\alpha - b_j + b_n)} P[y_n|\gamma]. \quad (36)$$

Note that this is equivalent as

$$\mathbf{s} = D^T \mathbf{v}^T, \quad (37)$$

where \mathbf{v} is an element that corresponds to matrix V . Next, we calculate \mathbf{g} , as

$$g_j(Z) = \sum_{\alpha \in \mathbb{Z}_4} Z^\alpha \sum_{\beta \in \mathbb{Z}_4} \frac{s_{j,\beta}}{r_{j,\beta}} \cdot r_{j,\beta - \alpha}. \quad (38)$$

After a simple analysis, we can see that

$$g_j(Z) = \sum_{\alpha \in \mathbb{Z}_4} Z^\alpha \sum_{\mathbf{b} \in \mathbb{C}^L} \prod_{n=0}^{N-1} \sum_{\gamma \in \mathbb{Z}_4} \omega^{-\gamma(b_n - b_j + \alpha \delta_{j,n})} P[y_n|\gamma]. \quad (39)$$

Next, with the help of (10), we obtain,

$$h_j(Z) = \sum_{\alpha \in \mathbb{Z}_4} Z^\alpha \sum_{\beta \in \mathbb{Z}_4} \omega^{-\alpha\beta} g_{j,\beta}. \quad (40)$$

Finally, we compute

$$z_j(Z) = \sum_{\alpha \in \mathbb{Z}_4} Z^\alpha \frac{h_{j,\alpha}}{4 \cdot m_j}, \quad (41)$$

where m_j is a scaling factor defined as

$$m_j = \sum_{\beta \in \mathbb{Z}_4} \frac{s_{j,\beta}}{r_{j,\beta}}. \quad (42)$$

This concludes the algorithm. It is easy to see that the complexity of this algorithm is the same as that of the Kerdock MAP decoding algorithm, i.e., $\mathcal{O}(N^2 \log_2 N)$. We summarize the MAP decoding of Preparata codes in Algorithm 3. A detailed complexity analysis of Algorithm 3 is given in Table II. Similar to the case of the Kerdock MAP decoder, all operations are done in \mathbb{S} . Note that the Fourier transform in eq. (29) also has complexity $4^2\mathcal{O}(1)$.

Algorithm 3 MAP decoding of Preparata codes

Input: y ,

Output: z

- 1: Compute the element of likelihoods \mathbf{w} using eq. (28).
 - 2: Compute the element \mathbf{r} using eq. (29).
 - 3: **for** $n = 0; n < N; n \leftarrow n + 1$ **do**
 - 4: $\rho_n \leftarrow \sum_{\alpha \in \mathbb{Z}_4} \log |r_{n,\alpha}| Z^\alpha$, {Using eq. (30)}
 - 5: $\phi_n(Z) \leftarrow \sum_{\alpha \in \mathbb{Z}_4} \arg\{r_{n,\alpha}\} Z^\alpha$ {Using eq. (31)}
 - 6: **end for**
 - 7: **for** $n = 0; n < N; n \leftarrow n + 1$ **do**
 - 8: $\mathbf{t}_n \leftarrow \text{FWHT}(\boldsymbol{\rho} \odot \bar{\mathbf{d}}_n^1)$
 - 9: $\mathbf{e}_n \leftarrow \text{FWHT}(\boldsymbol{\phi} \odot \bar{\mathbf{d}}_n^1)$
 - 10: **end for**
 - 11: **for** $n = 0; n < N; n \leftarrow n + 1$ **do**
 - 12: {Compute element $\mathbf{v}_n \in \mathbb{S}^N$ using eq. (34):}
 - 13: **for** $l = 0; l < N; l \leftarrow l + 1$ **do**
 - 14: $v_{n,l}(Z) \leftarrow \sum_{\alpha \in \mathbb{Z}^4} Z^\alpha \exp\{t_{n,l,\alpha}\} \cdot \exp\{e_{n,l,\alpha}\}$
 - 15: **end for**
 - 16: **end for**
 - 17: $\mathbf{s} \leftarrow \mathbf{0}$ {Initialize \mathbf{s} to the all-zero value}
 - 18: **for** $n = 0; n < N; n \leftarrow n + 1$ **do**
 - 19: $\mathbf{s} \leftarrow \mathbf{s} + \text{FWHT}(\mathbf{v}_n) \odot \bar{\mathbf{d}}_n^1$,
 - 20: **end for**
 - 21: Compute element \mathbf{g} using eq. (38).
 - 22: Compute element \mathbf{h} using \mathbf{g} and eq. (40).
 - 23: **for** $n = 0; n < N; n \leftarrow n + 1$ **do**
 - 24: $z_n(Z) \leftarrow \sum_{\alpha \in \mathbb{Z}_4} Z^\alpha \frac{h_{n,\alpha}}{4 \cdot m_n}$, {Using eq. (41) and (42)}
 - 25: **end for**
-

IV. BITWISE APP DECODING ALGORITHM

A linear block code over \mathbb{Z}_{p^k} (for some prime p and a positive integer k) with a p -adic expansion of the generator matrix $(G_0, G_1, \dots, G_{k-1})$, such that G_0 is of full rank over \mathbb{Z}_p , is called a splitting code [25]. The lifting decoder technique is a process of lifting a decoding scheme for the linear code over \mathbb{Z}_p , defined by the generator matrix G_0 to decoding schemes for the corresponding linear codes over \mathbb{Z}_{p^m} , $m = \{1, \dots, k\}$ [25, 26]. Instead of iteratively estimating the error element as done in [25, 26], we will define a residue that can easily be estimated at run-time and used to decode the codeword layer by layer.

Consider again the codeword $\mathbf{c} = \mathbf{u}G \in \mathbb{Z}_4^N$, with a dyadic expansion $(\mathbf{c}_0, \mathbf{c}_1)$. By substituting $G = G_0 + 2 \cdot G_1$ in eq. (17), we obtain

$$\mathbf{c} = \mathbf{u}_0 \cdot G_0 + 2 \cdot (\mathbf{u}_0 \cdot G_1 + \mathbf{u}_1 \cdot G_0). \quad (43)$$

Let $(\mathbf{r}_0, \mathbf{r}_1)$ represent the dyadic expansion of the residue part $\mathbf{u}_0 \cdot G_0$, with

$$\mathbf{r}_0 = \mathbf{u}_0 \otimes G_0, \quad (44)$$

and

$$\mathbf{r}_1 = \frac{\mathbf{u}_0 \cdot G_0 - \mathbf{u}_0 \otimes G_0}{2}. \quad (45)$$

By substituting this back into (43), we get

$$\mathbf{c} = \mathbf{u}_0 \otimes G_0 + 2 \cdot (\mathbf{r}_1 + \mathbf{u}_0 \cdot G_1 + \mathbf{u}_1 \cdot G_0). \quad (46)$$

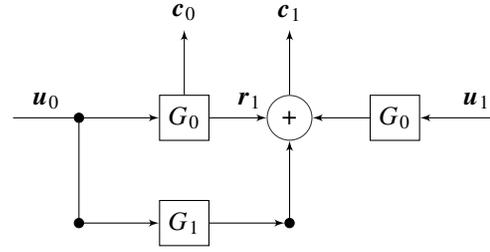


Fig. 1. Graphical representation of the encoder, defined by eq. (47).

Using [25, Lemma 1], we have

$$\mathbf{c} = \mathbf{u}_0 \otimes G_0 + 2 \cdot (\mathbf{r}_1 \oplus \mathbf{u}_0 \otimes G_1 \oplus \mathbf{u}_1 \otimes G_0) = \mathbf{c}_0 + 2 \cdot \mathbf{c}_1. \quad (47)$$

A graphical representation of the encoder is given in Fig. 1.

Given the channel output \mathbf{y} , we begin the decoding process by calculating reliability elements $\mathbf{w}_0, \mathbf{w}_1 \in \mathbb{R}^N$ as

$$w_{0,n} = \log \frac{P[y_n | c_{0,n} = 0]}{P[y_n | c_{0,n} = 1]}, \quad n = 0, 1, \dots, N-1, \quad (48)$$

and

$$w_{1,n} = \log \frac{P[y_n | c_{1,n} = 0]}{P[y_n | c_{1,n} = 1]}, \quad n = 0, 1, \dots, N-1. \quad (49)$$

Next, we compute $\mathbf{d}_0 \in \mathbb{R}^N$ as

$$\mathbf{d}_0 = D(\mathbf{w}_0), \quad (50)$$

where $D(\cdot)$ represents the SISO decoding algorithm corresponding to the binary linear block code, defined by the generator matrix G_0 . In the case of the Kerdock code, the corresponding binary code is the RM(1, m) code, while in the case of the Preparata code, the corresponding binary code is the extended Hamming code. Low complexity SISO decoding algorithms for these codes were presented in [36].

Given \mathbf{d}_0 it is easy to find the hard decision estimates $\hat{\mathbf{c}}_0$ and $\hat{\mathbf{u}}_0$. We calculate $\hat{\mathbf{r}}_1$ using eq. (45) and $\hat{\mathbf{p}}$ as

$$\hat{\mathbf{p}} = \hat{\mathbf{r}}_1 \oplus \hat{\mathbf{u}}_0 \otimes G_1. \quad (51)$$

Let $\mathbf{b} = \phi(\hat{\mathbf{p}})$, where $\phi(c) = 1 - 2c$ represents the BPSK modulation. Finally, we compute

$$\mathbf{d}_1 = D(\mathbf{b} \odot \mathbf{w}_1). \quad (52)$$

Elements \mathbf{d}_0 and $\mathbf{b} \cdot \mathbf{d}_1$ correspond to soft estimates of \mathbf{c}_0 and \mathbf{c}_1 , respectively. This concludes the algorithm.

As the decoder $D(\cdot)$ of the corresponding binary subcode has complexity $\mathcal{O}(N \log_2 N)$ [36] and assuming the calculation of $\hat{\mathbf{p}}$ (which has the same complexity as the encoding procedure) takes at most $\mathcal{O}(N \log_2 N)$, the lifting decoder also has complexity $\mathcal{O}(N \log_2 N)$. We summarize the APP decoding procedure in Algorithm 4. A detailed complexity analysis of Algorithm 4 for the case of Kerdock and Preparata codes is given in Table III. Note that operations are now done using floating-point numbers with some binary and quaternary computations in step 4 and 5.

Algorithm 4 Bitwise APP decoding algorithm

Input: y ,

Output: d_0, d_1

- 1: Compute the reliability element w_0 using eq. (48)
 - 2: Compute the reliability element w_1 using eq. (49)
 - 3: $d_0, \hat{u}_0 \leftarrow D(w_0)$
 - 4: $\hat{r}_1 \leftarrow (u_0 \cdot G_0 - u_0 \otimes G_0)/2$ {Using eq. (45)}
 - 5: $\hat{p} \leftarrow \hat{r}_1 \oplus \hat{u}_0 \otimes G_1$ {Using eq. (51)}
 - 6: $b \leftarrow \phi(\hat{p})$
 - 7: $d_1 \leftarrow D(b \odot w_1)$
-

 TABLE III
 COMPUTATIONAL COST OF BITWISE APP DECODING

Steps	Short description	Complexity
1. - 2.	Compute w_0 and w_1	$\mathcal{O}(N)$
3.	Decode w_0	$\mathcal{O}(N \log_2 N)$
4.	Calculate r_1	$\mathcal{O}(N \log_2 N)$
5.	Calculate \hat{p}	$\mathcal{O}(N \log_2 N)$
6.	BPSK modulation of \hat{p}	$\mathcal{O}(N)$
7.	Decode $w_1 \odot b$	$\mathcal{O}(N \log_2 N)$

V. SIMULATION RESULTS

We will now demonstrate the error-correcting performance of the new decoders introduced in section III and IV, for the case of four different Kerdock and Preparata codes of length⁵ 8, 32, 128 and 512, defined in terms of the irreducible monic polynomial ($h(Z)$) used to design an extension ring, as presented in Section II. These codes are the self-dual Nordstrom-Robinson code, defined by $h(Z) = 3 + Z + 2Z^2 + Z^3$, and Kerdock and Preparata codes over finite rings defined by $h(Z) = 3 + 2Z + 3Z^2 + Z^5$, $h(Z) = 3 + Z + 2Z^4 + Z^7$ and $h(Z) = 3 + 2Z^2 + 3Z^4 + Z^9$. All results are presented for the additive white Gaussian noise channel with a QPSK modulation. In the case of the MAP decoders, a standard QPSK modulation defined as $\phi(c) = I^c, c \in \mathbb{Z}_4$ is used, while in the case of the sub-optimal decoders we used a Gray-coded QPSK with respect to the dyadic expansion of a quaternary symbol. The performance of the proposed decoding algorithms is given in terms of the frame error rate (FER) and the symbol error rate (SER) as a function of the energy per bit to noise power spectral density ratio (E_b/N_0). In the case of the Nordstrom-Robinson code, we also provide the FER of a naive MAP decoder, implemented using eq. (5) (or eq. (10), as the Nordstrom-Robinson is self-dual and both equations give the same result) and show that it matches the two novel MAP decoders. We also compared our novel decoding algorithms with the classical lifting decoder [25] and the \mathbb{Z}_4 Chase decoder [41, 42] in terms of FER and SER. The original lifting decoder was implemented as a two stage decoder, where each stage used a binary hard decision decoder corresponding to the associated binary code. In the case of the Preparata codes we used the Meggitt decoder [52] and in the

⁵Note that the code length here is given as the number of quaternary symbols. The binary code length would be twice this.

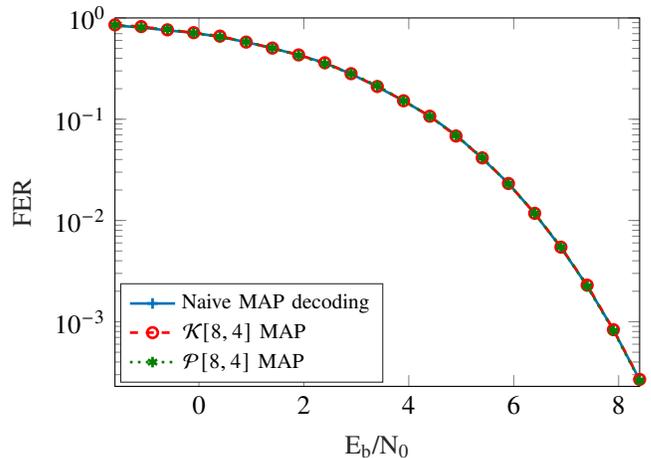


Fig. 2. FER comparison of different MAP decoders for the Nordstrom-Robinson code.

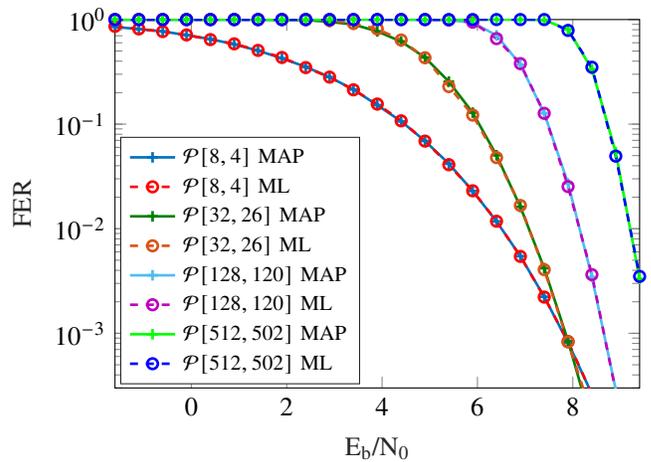


Fig. 3. FER comparison of the novel MAP decoding algorithm with an ML lower bound for different Preparata codes.

case of the Kerdock codes we used the minimum Hamming distance decoder. The \mathbb{Z}_4 Chase decoder improves upon the original lifting decoder by using the Chase reprocessing step at every stage, i.e. at stage $i \in \{1, 2\}$, the decoder generates 2^{e_i} binary test patterns of maximum Hamming weight e_i , where ones are restricted to the e_i least reliable positions in the corresponding channel output. Out of 2^{e_i} generated decoder outputs the one that minimizes the Euclidean distance is chosen as the correct one [42]. In the case of the Preparata codes we used parameters $e_1 = 2$ and $e_2 = 1$, while in the case of the Kerdock codes we used parameters $e_1 = 8$ and $e_2 = 4$.

All simulations are done using the Monte-Carlo simulation with a relative precision $\delta = 0.05$ for a range of E_b/N_0 points, starting from $-1.6dB$ with a step of $0.5dB$.

FER of the Nordstrom-Robinson code using the naive MAP decoder compared to the two novel MAP decoders is presented in Fig. 2. As expected, all three error-rate curves overlap. If the Euclidean distance between the correct codeword and the channel output is greater than the distance between the decoded sequence and the channel output, we assume that

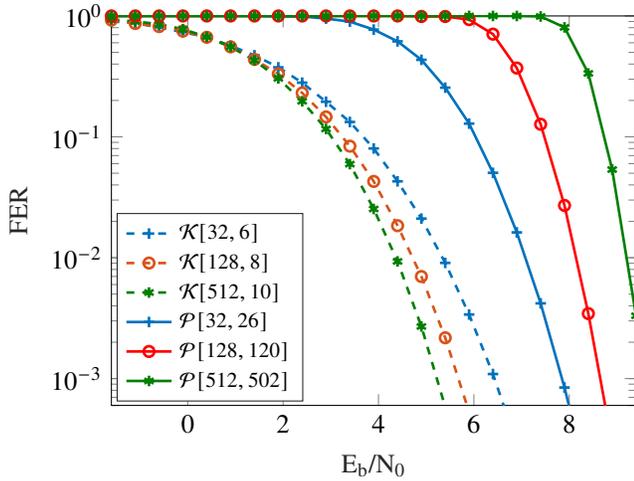


Fig. 4. FER comparison of different Kerdock and Preparata codes using the novel MAP decoding algorithms.

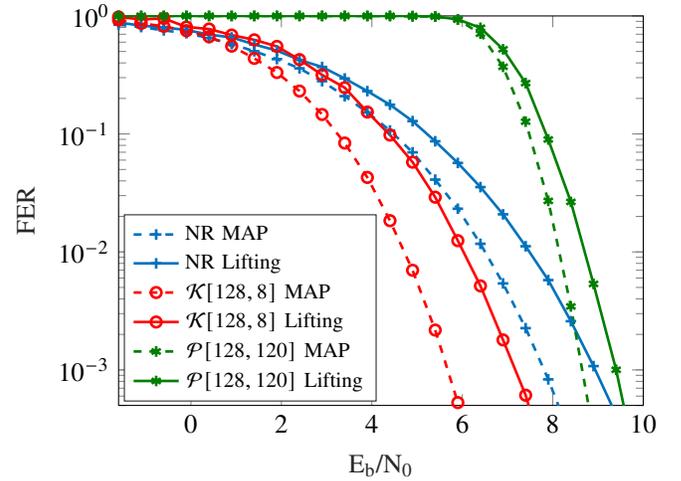


Fig. 6. FER of different Kerdock and Preparata codes using a sub-optimal decoder compared to the optimal MAP decoding.

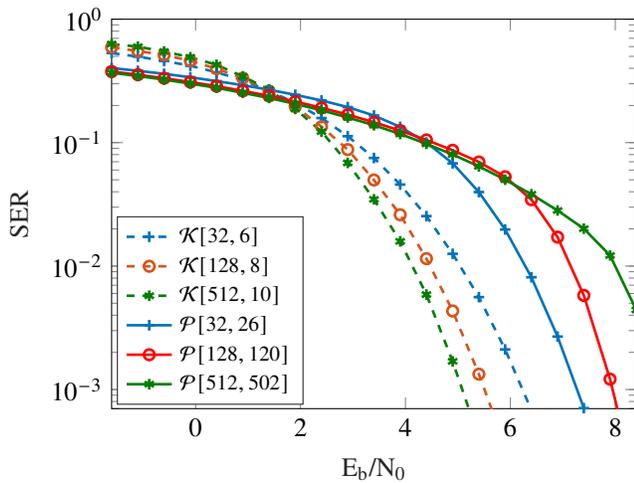


Fig. 5. SER comparison of different Kerdock and Preparata codes using the novel MAP decoding algorithms.

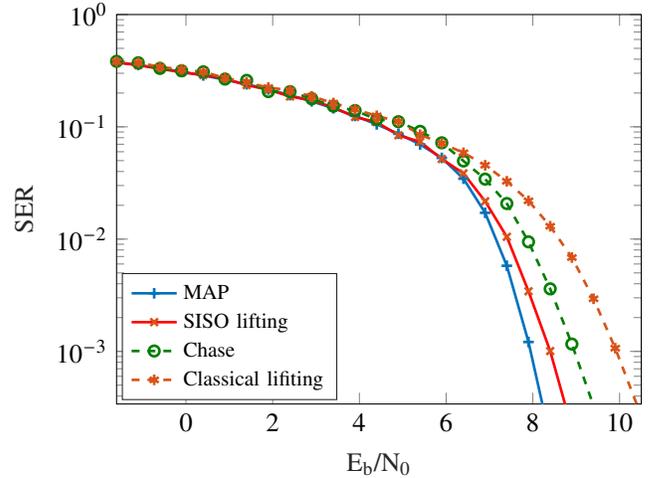


Fig. 7. SER comparison of the Preparata $\mathcal{P}[128, 120]$ code decoded using MAP, SISO lifting, Chase and classical lifting decoders.

the Maximum-Likelihood (ML) decoder would also make a mistake. This allows us to simulate the ML lower bound. In Fig. 3 it is shown that the FER performance of the MAP decoder perfectly coincides with the ML lower bound, for several different Preparata codes, as expected. FER of different Kerdock and Preparata codes using novel MAP decoders is presented in Fig. 4. SER of different Kerdock and Preparata codes using novel MAP decoders is presented in Fig. 5. Sub-optimal decoding of different Kerdock and Preparata codes compared to optimal decoding is presented in Fig. 6. Note that Kerdock and Preparata families are not fixed-rate sequences of codes, i.e. the code rate of Kerdock codes decreases with length, while the code rate of Preparata codes increases. It follows that the error-correcting performance of Kerdock codes increases with length, while the performance of Preparata codes decreases with length, as seen in Fig. 4 and Fig. 5.

SER performance of the $\mathcal{P}[128, 120]$ code using the MAP decoder, the sub-optimal SISO decoder, the \mathbb{Z}_4 Chase decoder and the classical lifting decoder is shown in Fig. 7. As

expected, the MAP decoder has the best performance, while the sub-optimal SISO decoder is better than the classical lifting and the Chase decoder. The MAP decoder has a coding gain of about $1dB$ and $2dB$ compared to the Chase and the classical lifting decoders, respectively. The sub-optimal SISO decoder has a coding gain of about $0.5dB$ and $1.5dB$ compared to the Chase and the classical lifting decoders, respectively. Different decoding algorithms are also compared in terms of FER and results for the case of the $\mathcal{K}[32, 6]$ code are shown in Fig. 8. The MAP decoder is optimal, so it has the best performance. We again notice that the sub-optimal SISO decoder is better than the classical lifting decoder and the Chase decoder. In the case of FER, the coding gain is more significant, and the MAP decoder achieves a coding gain of about $3dB$ compared to the Chase decoder.

VI. CONCLUSION

This paper introduces two novel low complexity MAP decoding algorithms for decoding Kerdock and Preparata codes.

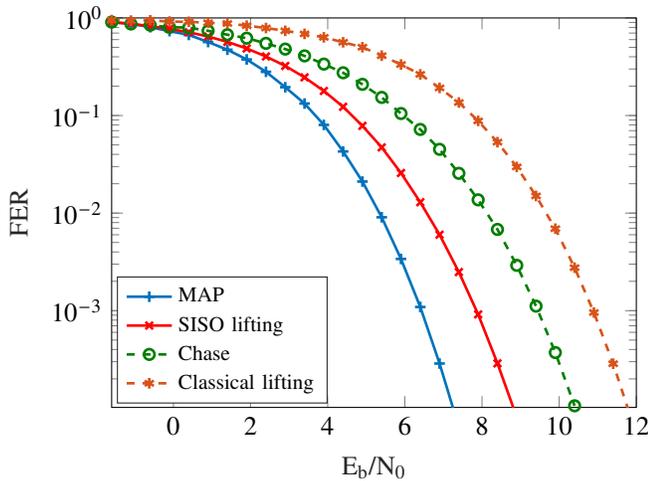


Fig. 8. FER comparison of the Kerdock $\mathcal{K}[32, 6]$ code decoded using MAP, SISO lifting, Chase and classical lifting decoders.

The complexity of these decoding algorithms is $O(N^2 \log_2 N)$. A sub-optimal bit-wise soft-decision decoding algorithm, based on the decoder lifting technique, with complexity $O(N \log_2 N)$ is also introduced. Compared to existing decoders, the novel decoders developed in this paper outperform existing ones in terms of error rate. Future work will deal with improving the error-correcting performance of the sub-optimal decoder, as well as developing new SISO decoders for other quaternary codes.

ACKNOWLEDGMENT

The authors are very grateful to the reviewers and the Editor, Prof. Li Chen, for their valuable comments that improved the quality and presentation of this paper.

REFERENCES

- [1] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Sole, "The z /₄-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Transactions on Information Theory*, vol. 40, no. 2, pp. 301–319, 1994.
- [2] A. Kerdock, "A class of low-rate nonlinear binary codes," *Information and Control*, vol. 20, no. 2, pp. 182 – 187, 1972. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0019995872903762>
- [3] F. P. Preparata, "A class of optimum nonlinear double-error-correcting codes," *Information and Control*, vol. 13, no. 4, pp. 378 – 400, 1968. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0019995868908747>
- [4] J. M. Goethals, "Two dual families of nonlinear binary codes," *Electronics Letters*, vol. 10, no. 23, pp. 471–472, 1974.
- [5] J.-M. Goethals, "Nonlinear codes defined by quadratic forms over $GF(2)$," *Information and Control*, vol. 31, no. 1, pp. 43 – 74, 1976. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0019995876903843>
- [6] P. Delsarte and J. Goethals, "Alternating bilinear forms over $GF(q)$," *Journal of Combinatorial Theory, Series A*, vol. 19, no. 1, pp. 26 – 50, 1975. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/0097316575900904>
- [7] A. W. Nordstrom and J. P. Robinson, "An optimum nonlinear code," *Information and Control*, vol. 11, no. 5, pp. 613 – 616, 1967. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0019995867908352>
- [8] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, ser. Grundlehren der mathematischen Wissenschaften. Springer, 1988, vol. 290.

- [9] H. Li, Z. Zou, X. Zhao, and K. Wang, "A novel soft-in-soft-out decoder for Nordstrom-Robinson code," in *2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2008, pp. 1213–1216.
- [10] Q. Xie, K. Peng, J. Wang, J. Song, J. Wang, and Z. Yang, "Low complexity soft decoder for Nordstrom-Robinson code with application to the Chinese DTTB standard," *IEEE Transactions on Broadcasting*, vol. 55, no. 3, pp. 668–673, 2009.
- [11] H. Kim, G. Markarian, and V. C. da Rocha Jr, "Nonlinear turbo product codes," in *XXV Simpósio Brasileiro de Telecomunicações*, 09 2007.
- [12] H. Kim, G. Markarian, and V. C. d. Rocha Jr., "Nonlinear product codes and their low complexity iterative decoding," *ETRI Journal*, vol. 32, no. 4, pp. 588–595, 2010. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.4218/etrij.10.0109.0643>
- [13] Takao Inoue and R. W. Heath, "Kerdock codes for limited feedback MIMO systems," in *2008 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2008, pp. 3113–3116.
- [14] T. Inoue and R. W. Heath, Jr., "Kerdock codes for limited feedback precoded MIMO systems," *IEEE Transactions on Signal Processing*, vol. 57, no. 9, pp. 3711–3716, 2009.
- [15] A. R. Calderbank, S. N. Diggavi, and N. Al-Dhahir, "Space-time signaling based on Kerdock and Delsarte-Goethals codes," in *2004 IEEE International Conference on Communications (IEEE Cat. No.04CH37577)*, vol. 1, 2004, pp. 483–487 Vol.1.
- [16] J. A. Davis and J. Jedwab, "Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes," *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp. 2397–2417, 1999.
- [17] K. Schmidt, "Quaternary constant-amplitude codes for multicode cdma," in *2007 IEEE International Symposium on Information Theory*, 2007, pp. 2781–2785.
- [18] I. Shakeel, "Performance of Reed-Muller and Kerdock coded MC-CDMA system with nonlinear amplifier," in *2005 Asia-Pacific Conference on Communications*, 2005, pp. 644–648.
- [19] O. Amrani, "Nonlinear codes: The product construction," *IEEE Transactions on Communications*, vol. 55, no. 10, pp. 1845–1851, 2007.
- [20] B. Karp, O. Amrani, and O. Keren, "Nonlinear product codes for reliability and security," in *2019 IEEE 4th International Verification and Security Workshop (IVSW)*, 2019, pp. 13–18.
- [21] T. Ninacs, B. Matuz, G. Liva, and G. Colavolpe, "Short non-binary low-density parity-check codes for phase noise channels," *IEEE Transactions on Communications*, vol. 67, no. 7, pp. 4575–4584, 2019.
- [22] K. Ravindran, A. Thangaraj, and S. Bhashyam, "LDPC codes for network-coded bidirectional relaying with higher order modulation," *IEEE Transactions on Communications*, vol. 63, no. 6, pp. 1975–1987, 2015.
- [23] R. Barrolleta, J. Pujol, and M. Villanueva, "Comparing decoding methods for quaternary linear codes," *Electronic Notes in Discrete Mathematics*, vol. 54, pp. 283 – 288, 2016, discrete Mathematics Days - JMDA16. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1571065316301433>
- [24] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*, ser. Mathematical Studies. Elsevier Science, 1977.
- [25] M. Greferath and U. Vellbinger, "Efficient decoding of z /_p-linear codes," *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 1288–1291, 1998.
- [26] N. S. Babu and K. Zimmermann, "Decoding of linear codes over Galois rings," *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1599–1603, 2001.
- [27] J. Conway and N. Sloane, "Soft decoding techniques for codes and lattices, including the Golay code and the Leech lattice," *IEEE Transactions on Information Theory*, vol. 32, no. 1, pp. 41–50, 1986.
- [28] R. D. Barrolleta and M. Villanueva, "Partial permutation decoding for binary linear and Z_4 -linear Hadamard codes," *Designs, Codes and Cryptography*, vol. 86, no. 3, pp. 569–586, Mar 2018. [Online]. Available: <https://doi.org/10.1007/s10623-017-0342-8>
- [29] R. D. Barrolleta and M. Villanueva, "Partial permutation decoding for several families of linear and Z_4 -linear codes," *IEEE Transactions on Information Theory*, vol. 65, no. 1, pp. 131–141, 2019.
- [30] J. P. Adoul, "Fast ML decoding algorithm for the Nordstrom - Robinson code (corresp.)," *IEEE Transactions on Information Theory*, vol. 33, no. 6, pp. 931–933, 1987.
- [31] A. Abbaszadeh and C. Rushforth, "Implementation of a fast maximum-likelihood decoding algorithm for the extended Nordstrom-Robinson code," *Integration*, vol. 13, no. 1, pp. 81 – 96, 1992. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/016792609290019U>
- [32] A. Vardy, "The Nordstrom-Robinson code: representation over $GF(4)$ and efficient decoding," *IEEE Transactions on Information Theory*,

vol. 40, no. 5, pp. 1686–1693, 1994.

- [33] M. Elia, C. Losana, and F. Neri, “Note on the complete decoding of Kerdock codes,” *IEE Proceedings I - Communications, Speech and Vision*, vol. 139, no. 1, pp. 24–28, 1992.
- [34] L. Bahl, J. Cocke, F. Jelinek, and J. Raviv, “Optimal decoding of linear codes for minimizing symbol error rate (corresp.),” *IEEE Transactions on Information Theory*, vol. 20, no. 2, pp. 284–287, 1974.
- [35] Y. Shany, I. Reuven, and Y. Be’ery, “On the trellis representation of the Delsarte-Goethals codes,” *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1547–1554, 1998.
- [36] A. Ashikhmin and S. Litsyn, “Simple MAP decoding of first-order Reed-Muller and Hamming codes,” *IEEE Transactions on Information Theory*, vol. 50, no. 8, pp. 1812–1818, 2004.
- [37] Yaron Shany and Y. Be’ery, “The Preparata and Goethals codes: trellis complexity and twisted squaring constructions,” *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1667–1673, 1999.
- [38] G. D. Forney, “Coset codes. II. binary lattices and related codes,” *IEEE Transactions on Information Theory*, vol. 34, no. 5, pp. 1152–1187, 1988.
- [39] B. Honary and G. Markarian, *Trellis Decoding of Block Codes: A Practical Approach*. USA: Kluwer Academic Publishers, 1997.
- [40] H. Kim, G. Markarian, and V. C. da Rocha, “Low complexity iterative decoding of product codes using a Generalized Array Code form of the Nordstrom-Robinson code,” in *2010 6th International Symposium on Turbo Codes Iterative Information Processing*, 2010, pp. 88–92.
- [41] M. A. Armand, “Chase decoding of linear z /₄ codes,” *Electronics Letters*, vol. 42, no. 18, pp. 1049–1050, 2006.
- [42] M. A. Armand, A. Halim, and A. Nallanathan, “Chase decoding of linear z /₄ codes at low to moderate rates,” *IEEE Communications Letters*, vol. 11, no. 10, pp. 811–813, 2007.
- [43] T. Helleseth and P. V. Kumar, “The algebraic decoding of the z /₄-linear Goethals code,” *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 2040–2048, 1995.
- [44] E. Byrne and P. Fitzpatrick, “Hamming metric decoding of alternant codes over Galois rings,” *IEEE Transactions on Information Theory*, vol. 48, no. 3, pp. 683–694, 2002.
- [45] Chunming Rong, T. Helleseth, and J. Lahtonen, “On algebraic decoding of the z /₄-linear Calderbank-McGuire code,” *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1423–1434, 1999.
- [46] K. Ranto, “On algebraic decoding of the z /₄-linear Goethals-like codes,” *IEEE Transactions on Information Theory*, vol. 46, no. 6, pp. 2193–2197, 2000.
- [47] Z. Wan, *Quaternary Codes*, ser. Series on applied mathematics. World Scientific Pub., 1997.
- [48] C. Hartmann and L. Rudolph, “An optimum symbol-by-symbol decoding rule for linear codes,” *IEEE Transactions on Information Theory*, vol. 22, no. 5, pp. 514–517, 1976.
- [49] J. Berkmann, “A symbol-by-symbol map decoding rule for linear codes over rings using the dual code,” in *Proceedings. 1998 IEEE International Symposium on Information Theory (Cat. No.98CH36252)*, 1998, p. 90.
- [50] J. Berkmann and C. Weiss, “On dualizing trellis-based app decoding algorithms,” *IEEE Transactions on Communications*, vol. 50, no. 11, pp. 1743–1757, 2002.
- [51] G. Forney, “Codes on graphs: Generalized state realizations,” 1999.
- [52] J. Meggitt, “Error correcting codes and their implementation for data transmission systems,” *IRE Transactions on Information Theory*, vol. 7, no. 4, pp. 234–244, 1961.



Vojin Šenk is Professor of Information Theory and Encoding Techniques, as well as High-tech Entrepreneurship at the University of Novi Sad, Serbia. Born in 1958, he received his B.Sc degree in Electrical Engineering from the University of Novi Sad in 1981, M.Sc and PhD in Electrical Engineering from the University of Belgrade in 1989 and 1992, respectively. He is interested in the efficient decoding of channel codes and their implementation.



Aleksandar Minja was born in Zrenjanin, Serbia, on June 19th 1987. He received the B.Sc (summa cum laude) and the M.Sc (summa cum laude) degrees in Electrical Engineering and Computer Science - Telecommunications Engineering and Signal Processing from the University of Novi Sad, Faculty of Engineering where he also finished his PhD and is currently working as an Assistant Professor. He is interested in channel coding and short packet communication.