

Chen L, Johnston M, Tian GY.

[Iterative Detection-Decoding of Interleaved Hermitian Codes for High Density Storage Devices.](#)

IEEE Transactions on Communications 2014, 62(10), 3401-3409

Copyright:

© 2014 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

DOI link to article:

<http://dx.doi.org/10.1109/TCOMM.2014.2357026>

Date deposited:

24/08/2016



This work is licensed under a [Creative Commons Attribution-NonCommercial 3.0 Unported License](#)

Iterative Detection-Decoding of Interleaved Hermitian Codes for High Density Storage Devices

Li Chen, *Senior Member, IEEE*, Martin Johnston, and Gui Yun Tian, *Senior Member, IEEE*

Abstract—Traditionally, Reed-Solomon (RS) codes have been employed in magnetic data storage devices due to their effectiveness in correcting random errors and burst errors caused by thermal asperities and inter-symbol interference (ISI). However, as storage densities increase the effect of ISI becomes more severe and much longer RS codes are needed, but this requires significantly increasing the size of the finite field. A possible replacement for RS codes are the one-point Hermitian codes, which are a class of algebraic-geometric (AG) code that have larger block sizes and minimum Hamming distances over the same finite field. In this paper, we present a novel iterative soft detection-decoding algorithm for interleaved Hermitian codes. The soft decoding employs a joint adaptive belief propagation (ABP) algorithm and Koetter-Vardy (KV) list decoding algorithm. It is combined with a maximum *a posteriori* (MAP) partial response (PR) equalizer and likelihoods from the output of the KV or the ABP algorithm are fed back to the equalizer. The proposed scheme's iterative detection-decoding behavior will be analyzed by utilizing the Extrinsic Information Transfer (ExIT) chart. Our simulation results demonstrate the performance gains achieved by iterations and Hermitian codes' performance advantage over RS codes.

Index Terms—Belief propagation, hermitian codes, iterative methods, Koetter-Vardy algorithm, partial response channel.

I. INTRODUCTION

ALGEBRAIC-GEOMETRIC (AG) codes were presented by Goppa in 1981 [1] and are a class of non-binary block codes constructed from the points on some affine curves. It is desirable to maximize the number of points as this results in AG codes with very long codewords and large minimum Hamming distances. For this reason, Hermitian curves are a popular choice of curve for constructing AG codes as one can achieve the maximal ratio between the number of affine points and its genus. Conventional Reed-Solomon (RS) codes can be viewed as the simplest type of AG code, constructed from the points on an affine line. However, the length of RS codewords is limited by the size of the finite field it is defined in since generally there are fewer points on an affine line than an affine curve. Johnston *et al.* [2] evaluated the performance of Hermitian codes using Sakata's algorithm [3] and showed that significant coding gains could be achieved over RS codes defined in the same finite field. Further improvements in

performance can be achieved with list decoding by using the Guruswami-Sudan (GS) algorithm [4], which can correct errors beyond the half distance bound. Hoholdt *et al.* [5] presented a list decoding algorithm for Hermitian codes by defining the interpolation property of a trivariate polynomial that is defined over the pole basis of a Hermitian curve. Chen *et al.* [6] were the first to evaluate the list decoding performance of Hermitian codes and at the same time presented a method to reduce the decoding complexity. GS algorithm was later modified by Koetter and Vardy [7] to obtain a soft-decision list decoding algorithm for RS codes, known as the Koetter-Vardy (KV) algorithm. Chen *et al.* [8] and Lee *et al.* [9] then independently developed a KV algorithm for Hermitian codes outperforming GS algorithm. Recently, Chen showed how the iterative decoding of Hermitian codes could be achieved by proposing the serial concatenation of an inner adaptive belief propagation (ABP) algorithm and an outer KV algorithm [10]. The ABP algorithm operates on an adapted binary parity-check matrix of a Hermitian code and enhances the reliability of the soft received information [11].

Due to a Hermitian code's very large minimum Hamming distance, it is ideally suited to channels that exhibit many burst errors and random errors, such as magnetic storage channels. Interleaved Hermitian codes comprise a number of Hermitian codewords interleaved using a block interleaver, allowing the codewords to assist each other during the decoding process. The codeword length is also effectively increased without increasing the size of finite field. In this paper, a turbo-like iterative detection-decoding scheme that integrates maximum *a posteriori* (MAP) [12] channel equalization and iterative soft decoding [10] of interleaved Hermitian codes is designed for partial response (PR) channels. The application of turbo equalization to magnetic storage channels is a well-known technique for the joint detection and decoding of read data and is commonly performed using the low-density parity-check (LDPC) codes [13] [14]. Although LDPC codes perform well with turbo equalization on magnetic channels, they are susceptible to error floors at low bit-error rates (BER) and since they are binary they are not as effective at correcting burst errors. Our proposed iterative decoding algorithm has been designed so that extrinsic likelihoods from the ABP algorithm and the decoded estimates from the KV algorithm are fed back to the trellis-based equalizer to form a loop. This significantly improves the code's error correction performance yielding significant coding gains over separate trellis-based equalization and Hermitian decoding. Approaches to improve the performance of the ABP-KV decoder will be introduced. The proposed scheme's iterative behavior will be analyzed by the Extrinsic Information Transfer (ExIT) chart [15] predicting

Li Chen is with the School of Information Science and Technology, Sun Yat-sen University, Guangzhou, China, e-mail: chenli55@mail.sysu.edu.cn, website: sist.sysu.edu.cn/~chenli.

Martin Johnston and Gui Yun Tian are with the School of Electrical and Electronic Engineering, Newcastle University, Newcastle-upon-Tyne, UK, e-mail: martin.johnston@ncl.ac.uk, g.y.tian@ncl.ac.uk

This work is supported by the National Natural Science Foundation of China (NSFC) with project ID 61372079, the National Basic Research Program of China (973 Program) with project ID 2012CB316100 and the EU 7th Framework Programme project Health Monitoring of Offshore Wind Farms (HEMOW).

the iterative error correction performance. The interleaved Hermitian codes' performance advantage over interleaved RS codes will also be demonstrated by simulations. It is important to point out that due to the presence of the outer KV algorithm there will be no error floor, unlike LDPC and turbo codes, highlighting the suitability of Hermitian codes for use with data storage channels.

The rest of the paper is organized as follows. Section II presents preliminary knowledge. Section III presents the proposed iterative detection-decoding scheme. Section IV analyzes the iterative scheme utilizing the ExIT chart. Sections V and VI analyze the performance and complexity of the proposal, respectively. Finally, Section VII concludes the paper.

II. PREREQUISITE KNOWLEDGE

This section presents prerequisite knowledge for the later sections of the paper, including the encoding of interleaved Hermitian codes and the PR channels.

A. Encoding

Let $\mathbb{F}_q = \{0, 1, \alpha, \dots, \alpha^{q-2}\}$ denote a finite field of size q where α is a primitive element of the field. Let $\mathbb{F}_q[x, y]$ and $\mathbb{F}_q[x, y, z]$ denote the rings of bivariate and trivariate polynomials defined over \mathbb{F}_q , respectively. In this paper, it is assumed that \mathbb{F}_q is an extension field of \mathbb{F}_2 such that $q = 2^\zeta$, where ζ is a positive even integer. The projective Hermitian curve defined in \mathbb{F}_q is:

$$H_w(x, y, z) = x^{w+1} + y^w z + yz^w, \quad (1)$$

where $w = \sqrt{q}$. A one-point Hermitian code is constructed from one of the projective curve's affine components $H_w(x, y, 1) = x^{w+1} + y^w + y$. There are $n = w^3 = q^{\frac{3}{2}}$ affine points that satisfy $H_w(x, y, 1) = 0$, which are of the form $p_j = (x_j, y_j, 1)$ ($1 \leq j \leq n$), and a point at infinity $p_\infty = (0, 1, 0)$. A pole basis Φ_w comprising monomials $\phi_a = \frac{x^\vartheta y^\lambda}{z^{\vartheta+\lambda}}$ is defined on $H_w(x, y, z)$ at p_∞ , where a is the index of ϕ_a in an ordered list of monomials and $(a, \vartheta, \lambda) \in \mathbb{N}^2$ and \mathbb{N} denotes the set of non-negative integers. In particular, $\vartheta \leq w$. With $H_w(x, y, z) = 0$, we have

$$\frac{x}{z} = \frac{y^w + yz^{w-1}}{x^w}, \quad \frac{y}{z} = \frac{y^{w+1} + y^2 z^{w-1}}{x^{w+1}}. \quad (2)$$

The order of the monomials $\frac{x}{z}$ and $\frac{y}{z}$ at the point at infinity, o_{p_∞} , becomes obvious with $o_{p_\infty}(\frac{x}{z}) = w$ and $o_{p_\infty}(\frac{y}{z}) = w + 1$. Therefore, the pole order of any monomial in Φ_w is $o_{p_\infty}(\frac{x^\vartheta y^\lambda}{z^{\vartheta+\lambda}}) = w\vartheta + (w+1)\lambda$. With $z = 1$ in the affine plane, the monomials ϕ_a in the pole basis Φ_w can be expressed just in terms of x and y . They are ordered in terms of increasing pole order and Φ_w can be defined as [3] [6]

$$\Phi_w = \{\phi_a | o_{p_\infty}(\phi_a) < o_{p_\infty}(\phi_{a+1}), \vartheta \leq w, a \in \mathbb{N}\}, \quad (3)$$

where the x -degree ϑ in all monomials ϕ_a is constrained to be less than the x -degree of the affine Hermitian curve, $w + 1$, to ensure the generator matrix has independent rows. The generator matrix $\mathbf{G} \in \mathbb{F}_q^{k \times n}$ of an (n, k) Hermitian code is obtained by evaluating the first k monomials in Φ_w at all $n = q^{\frac{3}{2}}$ affine points following [3]

$$\mathbf{G} = \begin{bmatrix} \phi_0(p_1) & \phi_0(p_2) & \dots & \phi_0(p_n) \\ \phi_1(p_1) & \phi_1(p_2) & \dots & \phi_1(p_n) \\ \vdots & \vdots & \ddots & \vdots \\ \phi_{k-1}(p_1) & \phi_{k-1}(p_2) & \dots & \phi_{k-1}(p_n) \end{bmatrix}, \quad (4)$$

where n is the length and k becomes the dimension of the code. Encoding of a message vector $\overline{F} = [F_1 F_2 \dots F_k] \in \mathbb{F}_q^k$ is achieved by $\overline{C} = \overline{F} \cdot \mathbf{G} = [C_1 C_2 \dots C_n] \in \mathbb{F}_q^n$. In order to perform the ABP decoding, the code's parity-check matrix needs to be known, and it is given as [3]

$$\mathbf{H} = \begin{bmatrix} \phi_0(p_1) & \phi_0(p_2) & \dots & \phi_0(p_n) \\ \phi_1(p_1) & \phi_1(p_2) & \dots & \phi_1(p_n) \\ \vdots & \vdots & \ddots & \vdots \\ \phi_{n-k-1}(p_1) & \phi_{n-k-1}(p_2) & \dots & \phi_{n-k-1}(p_n) \end{bmatrix}. \quad (5)$$

Given that $\xi(x) \in \mathbb{F}_2[x]$ is the minimal polynomial of α over \mathbb{F}_q , and Ξ is its companion matrix [16] with size $\zeta \times \zeta$, the binary image of matrix \mathbf{H} can be generated by mapping its entries $\alpha^i \mapsto \Xi^i$, where $i = 0, 1, \dots, q - 2$. This results in the binary parity-check matrix \mathbf{H}_b of the code with size $(n - k)\zeta \times n\zeta$.

Let Λ denote the depth of the block interleaver. After Λ independent Hermitian codewords $\overline{C}^{(1)}, \overline{C}^{(2)}, \dots, \overline{C}^{(\Lambda)}$ have been generated, they will then be interleaved according to the interleaving pattern that writes in symbols vertically and reads the symbols out horizontally, yielding the interleaved Hermitian codewords. They are then converted into binary interleaved coded bit sequences to be written onto the disc. We use c_t to denote the coded bits of a Hermitian codeword and $t = 1, 2, \dots, n\zeta$, and c'_t to denote the interleaved Hermitian coded bits. Since they are the binary outcome after interleaving Λ Hermitian codewords, for c'_t , $t = 1, 2, \dots, \Lambda n\zeta$.

B. Partial Response Channels

The demand for increasing the storage capacity of magnetic discs requires the packing of more data onto each square inch of the disc. When reading the data, the readback head detects changes in magnetic flux due to changes in the polarity of the write current. The output voltage from the readback head is a positive or negative pulse depending on whether the change in magnetic flux is positive or negative. In longitudinal recording, the transition response is commonly modelled as a Lorentzian pulse [17], whereas in perpendicular recording, the transition response can be modelled using a hyperbolic tangent [18]. For a fixed pulse width, inter-symbol interference (ISI) will increase as the density of recorded bits increases. For magnetic read channels ISI is not eliminated but it is actually shaped by a linear equalizer to have a predetermined response defined by a simple PR polynomial [19] so that ISI is still present after equalization. Given a symbol duration T and channel bandwidth B , the maximum transmission rate for binary signalling with no ISI is $\frac{1}{T} = 2B$ [17]. But this cannot be achieved with practical filters. However, if some ISI is still present then the maximum transmission rate of $2B$ symbols/sec. can be achieved.

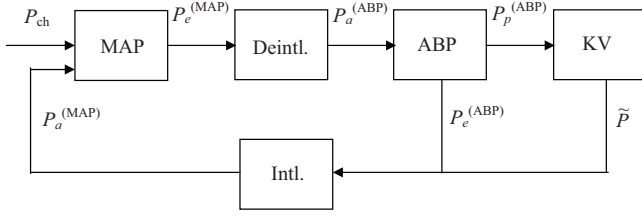


Fig. 1. Structure of the iterative detection-decoding scheme.

In this paper, we consider the perpendicular recording channels since it is now the recording method used in modern hard drives. The PR polynomials for perpendicular recording channels are $G(D) = (1 + D)^\varrho$, where D is a delay unit and ϱ is a positive integer, with a larger value of ϱ indicating more severe ISI. In the rest of the paper, the perpendicular channels that are modelled with the PR polynomials of $G(D) = \frac{1}{\sqrt{6}} + \frac{2}{\sqrt{6}}D + \frac{1}{\sqrt{6}}D^2$ and $G(D) = \frac{1}{\sqrt{20}} + \frac{3}{\sqrt{20}}D + \frac{3}{\sqrt{20}}D^2 + \frac{1}{\sqrt{20}}D^3$ are labelled PR channel I and PR channel II, respectively. The PR polynomials' coefficients ensure there is no channel gain. The linear equalizer is designed to minimize the mean squared error (MSE) between the equalized output and the desired output from the PR polynomial [19]. If the MSE is zero, the magnetic channel and equalizer are equivalent to a channel defined by the PR polynomial. Hence, by making the assumption that the equalized output and desired output are identical then for simulation purposes we can replace the magnetic channel and equalizer with a PR channel to obtain an ideally equalized signal with a controlled amount of ISI. The interleaved coded bits $c'_t \in \{0, 1\}$ are mapped to an NRZ signal $x_t \in \{-1, +1\}$. The output of the PR channels r_t is then obtained by first convolving x_t with the impulse response of the PR channel h_t and finally adding additive white Gaussian noise (AWGN) η_t with variance $\sigma^2 = \frac{N_0}{2}$ and N_0 is the noise power, i.e.,

$$r_t = x_t * h_t + \eta_t. \quad (6)$$

III. ITERATIVE DETECTION-DECODING

The iterative detection-decoding scheme is shown in Fig.1, where the detection and decoding are accomplished by the MAP and the ABP-KV algorithms, respectively. With the channel observations P_{ch} , the MAP detection determines the extrinsic probability $P_e^{(MAP)}$ of the interleaved Hermitian coded bits c'_t and $t = 1, 2, \dots, \Lambda n\zeta$. They are then deinterleaved and mapped to the *a priori* probabilities $P_a^{(ABP)}$ of the coded bits c_t of each Hermitian codeword and $t = 1, 2, \dots, n\zeta$. For each Hermitian codeword, the ABP algorithm delivers both the extrinsic probabilities $P_e^{(ABP)}$ and the *a posteriori* probabilities $P_p^{(ABP)}$ for the coded bits. With $P_p^{(ABP)}$, the KV algorithm further decodes the message. If KV decoding yields a message candidate, the deterministic probabilities \tilde{P} of the Hermitian coded bits will be fed back. Otherwise, the extrinsic probabilities $P_e^{(ABP)}$ will be fed back. They are then interleaved and mapped back to the *a priori* probabilities of the interleaved Hermitian coded bits $P_a^{(MAP)}$ for the next round MAP detection.

A. MAP Detection

PR equalization is achieved using the MAP algorithm [12]. The trellis-based equalizer is a component of the proposed iterative scheme and takes the *a priori* probabilities $P_a^{(MAP)}(c'_t)$ from either the ABP or KV decoder. Initially, no information is provided by the decoder and the *a priori* probabilities are initialized as $P_a^{(MAP)}(c'_t = 0) = P_a^{(MAP)}(c'_t = 1) = 0.5$. The PR channel has a binary input $c'_t \in \{0, 1\}$ and a real output r_t . The branch metrics $\gamma_t(s, s')$ of the MAP algorithm corresponding to the state transitions in the trellis diagram are

$$\gamma_t(s, s') = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(r_t - x(s, s'))^2}{\sigma^2}} \cdot P_a^{(MAP)}(c'_t), \quad (7)$$

where $x(s, s')$ denotes the trellis output for a transition from an initial state s to the next state s' and $x(s, s') \in \{-1, 1\}$. The MAP equalizer generates the likelihoods $P(c'_t|r_t)$ of the interleaved coded bits c'_t and the extrinsic probabilities $P_e^{(MAP)}(c'_t)$ are obtained from

$$P_e^{(MAP)}(c'_t) = \mathcal{N} \frac{P(c'_t|r_t)}{P_a^{(MAP)}(c'_t)}, \quad (8)$$

where $\mathcal{N} = \sum_{c'_t \in \{0, 1\}} P_e^{(MAP)}(c'_t)$ is a normalization factor. They are then deinterleaved and passed to the ABP-KV decoder. Since a codeword symbol can be decomposed into ζ bits, every ζ pairs of extrinsic probabilities ($P_e^{(MAP)}(c'_t = 0), P_e^{(MAP)}(c'_t = 1)$) that correspond to a codeword symbol are grouped together during the deinterleaving process.

B. ABP Decoding

The decoding of a Hermitian code is accomplished by the ABP-KV algorithm [10]. The ABP decoding enhances the bit-wise reliability information for KV decoding. Furthermore, it delivers the extrinsic probabilities of the Hermitian coded bits for the iterative detection-decoding.

After deinterleaving, and by reading out each row of the deinterleaver, the following mapping is realized

$$P_e^{(MAP)}(c'_t) \mapsto P_a^{(ABP)}(c_t), \quad (9)$$

and the *a priori* probability for each coded bit c_t of a Hermitian codeword can be obtained, where $t = 1, 2, \dots, n\zeta$. The *a priori* log-likelihood ratio (LLR) of c_t is determined by

$$L_{a,t} = \ln \left(\frac{P_a^{(ABP)}(c_t = 0)}{P_a^{(ABP)}(c_t = 1)} \right), \quad (10)$$

and the *a priori* LLR vector of a Hermitian codeword is

$$\bar{L}_a = [L_{a,1} \ L_{a,2} \ \dots \ L_{a,(n-k)\zeta} \ \dots \ L_{a,n\zeta}]. \quad (11)$$

The high density of 1s in \mathbf{H}_b of the Hermitian code must be reduced before belief propagation (BP) decoding starts. This is achieved by the bit reliability oriented Gaussian elimination. Since a higher magnitude of $|L_{a,t}|$ implies the bit is more reliable, the ABP algorithm sorts the *a priori* LLR values according to their magnitudes, yielding an updated bit index sequence $\delta_1, \delta_2, \dots, \delta_{(n-k)\zeta}, \dots, \delta_{n\zeta}$. It implies $|L_{a,\delta_1}| < |L_{a,\delta_2}| < \dots < |L_{a,\delta_{(n-k)\zeta}}| < \dots < |L_{a,\delta_{n\zeta}}|$ and bits $c_{\delta_1}, c_{\delta_2}, \dots, c_{\delta_{(n-k)\zeta}}$ are the $(n-k)\zeta$ least reliable bits. Let

$\Theta = \{\delta_1, \delta_2, \dots, \delta_{(n-k)\zeta}\} \subseteq \{1, 2, \dots, n\zeta\}$ denote the set of unreliable bit indices and $|\Theta| = (n-k)\zeta$. Its complementary set is $\Theta^c = \{\delta_{(n-k)\zeta+1}, \delta_{(n-k)\zeta+2}, \dots, \delta_{n\zeta}\}$. Based on Θ , the sorted *a priori* LLR vector becomes

$$\bar{L}_a^\Theta = [L_{a,\delta_1} \ L_{a,\delta_2} \ \dots \ L_{a,\delta_{(n-k)\zeta}} \ \dots \ L_{a,\delta_{n\zeta}}]. \quad (12)$$

Gaussian elimination will be performed on the matrix \mathbf{H}_b , reducing the columns that correspond to the unreliable bits to weight-1 columns. Let Υ_δ denote the weight-1 column vector with 1 at its δ th entry and 0 elsewhere. For matrix \mathbf{H}_b , Gaussian elimination reduces column δ_1 to Υ_1 , then reduces column δ_2 to Υ_2 , and etc. Gaussian elimination reduces the first $(n-k)\zeta$ independent columns implied by \bar{L}_a^Θ to weight-1 columns, resulting in an adapted parity-check matrix \mathbf{H}'_b with which the BP decoding is performed. Let $h_{ut} \in \{0, 1\}$ denote the entry of matrix \mathbf{H}'_b and $\mathbf{U}(t) = \{u \mid h_{ut} = 1, \forall 1 \leq u \leq (n-k)\zeta\}$ and $\mathbf{T}(u) = \{t \mid h_{ut} = 1, \forall 1 \leq t \leq n\zeta\}$. The iterative BP process is performed based on the Tanner graph defined by \mathbf{H}'_b , yielding the extrinsic LLR value for each Hermitian coded bit by

$$L_{e,t} = \sum_{u \in \mathbf{U}(t)} 2 \tanh^{-1} \left(\prod_{\tau \in \mathbf{T}(u) \setminus t} \tanh \left(\frac{L_{a,\tau}}{2} \right) \right). \quad (13)$$

After a number of BP iterations, the *a posteriori* LLR of each Hermitian coded bit can be determined by

$$L_{p,t} = L_{a,t} + \varphi L_{e,t}, \quad (14)$$

where $\varphi \in (0, 1]$ is the damping factor (DF). Therefore, the *a posteriori* LLR vector of a Hermitian codeword is

$$\bar{L}_p = [L_{p,1} \ L_{p,2} \ \dots \ L_{p,(n-k)\zeta} \ \dots \ L_{p,n\zeta}]. \quad (15)$$

In order to reduce the BP decoding complexity, the Min-Sum algorithm can be utilized with the extrinsic LLRs defined by

$$L_{e,t} = \sum_{u \in \mathbf{U}(t)} \left(\prod_{\tau \in \mathbf{T}(u) \setminus t} \text{sign}(L_{a,\tau}) \cdot \min_{\tau \in \mathbf{T}(u) \setminus t} \{|L_{a,\tau}|\} \right), \quad (16)$$

where for any $\psi \in \mathbb{R}$, $\text{sign}(\psi) = 1$ if $\psi \geq 0$, or $\text{sign}(\psi) = -1$ otherwise. The Min-Sum algorithm is more effective in decoding long Hermitian codes because the matrix \mathbf{H}'_b of these long codes still has a large number of short cycles¹, which affects the extrinsic LLR calculation in (13).

It can be seen that the ABP algorithm reduces the columns that correspond to the unreliable bits to weight-1 columns. Consequently, it prevents the propagation of the unreliable information during the BP calculation. With the assistance of the reliable information, the LLR values of the unreliable bits are likely to be improved. Note that there can be multiple Gaussian eliminations. If so, the *a posteriori* LLR vector needs to be mapped to the *a priori* LLR vector by $\bar{L}_p \mapsto \bar{L}_a$. The next round of bit reliability sorting and Gaussian elimination will be performed based on the updated \bar{L}_a . As a result, the ABP decoding becomes iterative. Each ABP iteration consists of bit reliability sorting, Gaussian elimination and BP decoding which is also iterative. Together with the iterative detection-decoding, there are three types of iterations in the

proposed scheme. We call the detection-decoding iteration as the global iteration and use N_1 , N_2 and N_3 to denote the designed number of global iteration, ABP iteration and BP iteration, respectively.

The extrinsic and *a posteriori* probabilities of the Hermitian coded bits can be further determined by

$$P_e^{(\text{ABP})}(c_t = 0) = \frac{1}{1 + e^{-L_{e,t}}}, \quad P_e^{(\text{ABP})}(c_t = 1) = \frac{1}{1 + e^{L_{e,t}}}, \quad (17)$$

$$P_p^{(\text{ABP})}(c_t = 0) = \frac{1}{1 + e^{-L_{p,t}}}, \quad P_p^{(\text{ABP})}(c_t = 1) = \frac{1}{1 + e^{L_{p,t}}}. \quad (18)$$

C. KV Decoding

With the *a posteriori* probabilities of (18), a $q \times n$ reliability matrix $\mathbf{\Pi}$ for each Hermitian codeword can be formed. Its entry π_{ij} is the symbol wise *a posteriori* probability and

$$\pi_{ij} = P_p(C_j = \rho_i), \quad (19)$$

where $\rho_i \in \mathbb{F}_q$ with $i = 1, 2, \dots, q$ and $j = 1, 2, \dots, n$. During the formation, ζ pairs of *a posteriori* probability values ($P_p^{(\text{ABP})}(c_t = 0), P_p^{(\text{ABP})}(c_t = 1)$) that correspond to a codeword symbol will be multiplied by q different permutations, yielding a column of matrix $\mathbf{\Pi}$. It will then be proportionally transformed into a multiplicity matrix \mathbf{M} of the same size and its entries $m_{ij} \in \mathbb{N}$ [7]. The interpolation process is dependent on the entries of \mathbf{M} , yielding a polynomial $Q \in \mathbb{F}_q[x, y, z]$ that interpolates each point (p_j, ρ_i) with a multiplicity of m_{ij} [8]. In general, $Q = \sum_{a,b} Q_{ab} \phi_a z^b$ and its x -degree is confined within w by the property of the affine curve, i.e. $x^{w+1} = y^w + y$. Finally, factorization is performed to find the z -roots of Q , delivering [20] [21]

$$\mathcal{L} = \{f \in \mathbb{F}_q[x, y] \mid Q(x, y, f) = 0\}. \quad (20)$$

The coefficients of f form a decoded message vector, which becomes a candidate in the decoding output list \mathcal{L} . Let $l = \deg_z Q$ denote the designed factorization output list size, and $|\mathcal{L}| \leq l$. It determines the error correction capability of KV decoding. Since KV decoding is performed after each ABP iteration, the ABP-KV decoding of a Hermitian codeword will provide at most lN_2 message candidates among which the maximum likelihood (ML) criterion will be utilized to select the decoding output. However, notice that in practice, the decoding output list \mathcal{L} often contains only a single candidate. If the KV algorithm provides a decoding output, the deterministic probabilities of the corresponding Hermitian coded bits can be obtained. Let $\hat{c}_t \in \{0, 1\}$ denote estimation of the decoded bit, the deterministic probability of bit c_t is determined by

$$\begin{cases} \tilde{P}(c_t = 0) = 1, \tilde{P}(c_t = 1) = 0, & \text{if } \hat{c}_t = 0; \\ \tilde{P}(c_t = 0) = 0, \tilde{P}(c_t = 1) = 1, & \text{if } \hat{c}_t = 1. \end{cases} \quad (21)$$

D. ABP-KV Decoding Feedback

Summarizing the above mentioned ABP-KV decoding, Fig.2 shows its functional steps and the probabilities that are being iterated. Moreover, the global, ABP and BP iterations are also indicated with their designed iteration numbers.

After KV decoding of all the Λ Hermitian codes, deterministic probabilities \tilde{P} of the decoded bits and extrinsic

¹In the adapted matrix \mathbf{H}'_b of the (512, 460) Hermitian code, the amount of short cycles will be around 1.15×10^{10} .

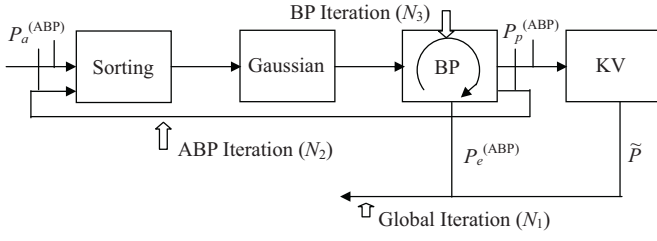


Fig. 2. Functional steps of the ABP-KV decoding.

probabilities $P_e^{(ABP)}$ of the undecoded bits will be given as feedback for the next round of MAP detection. After interleaving, they are mapped back to the *a priori* probabilities $P_a^{(MAP)}$ of the interleaved Hermitian coded bits as

$$P_e^{(ABP)}(c_t), \tilde{P}(c_t) \mapsto P_a^{(MAP)}(c'_t). \quad (22)$$

Note that for c'_t , $t = 1, 2, \dots, \Lambda n\zeta$. Hence, the next round of MAP detection functions with a portion of known *a priori* information, which helps to yield a more accurate detection outcome. At the same time, the extrinsic probabilities of the undecoded bits will be further iterated, allowing them to be decoded in later iterations. The iterative scheme terminates once all Λ Hermitian codewords have been decoded, or the designed global iteration number N_1 is reached. The decoded Hermitian codeword will not be decoded again in the following iterations. Hence, the next time MAP detection runs, only the extrinsic probabilities of the undecoded bits will be determined by (8). This requires the system to know the identities of the undecoded bits. We can use a binary indicator of size $\Lambda n\zeta$ indicating each coded bit's decoding status. Information of the indicator will also be interleaved alongside the probabilities $P_e^{(ABP)}(c_t)$, $\tilde{P}(c_t)$, so that the MAP detector knows the identity of the undecoded bits.

E. Performance Improvement Approaches

The performance of the iterative detection-decoding scheme can be further improved by strengthening the ABP-KV decoding and more Hermitian codewords can be decoded within an iteration, feeding back more known *a priori* information for the MAP detection. To improve KV decoding performance, we can increase the designed factorization output list size l [8]. To improve the ABP decoding performance, we can try to restructure the unreliable bit indices group Θ , spinning out a number of independent ABP-KV decodings. E.g., with $\chi < \min\{k\zeta, (n-k)\zeta\}$, we can restructure Θ as $\Theta = \{\delta_{(n-k)\zeta+1}, \dots, \delta_{(n-k)\zeta+\chi}, \delta_1, \dots, \delta_{(n-k)\zeta-\chi}\}$. The sorted *a priori* LLR vector \bar{L}_a^Θ becomes

$$\bar{L}_a^\Theta = [L_{a, \delta_{(n-k)\zeta+1}} \cdots L_{a, \delta_{(n-k)\zeta-\chi}} \quad L_{a, \delta_{(n-k)\zeta-\chi+1}} \cdots L_{a, \delta_{(n-k)\zeta}} \quad L_{a, \delta_{(n-k)\zeta+\chi+1}} \cdots L_{a, \delta_{n\zeta}}]. \quad (23)$$

The following Gaussian elimination will be performed based on the above sorted vector. Such an attempt is proposed based on the observation that the Hermitian coded bits of the original set Θ^c can also be wrongly estimated by their LLR values. With their corresponding columns being reduced to weight-1, they are granted an opportunity to be corrected by the BP decoding. Details of such an approach can be found in [10].

IV. EXIT CHART INSIGHTS

This section utilizes the EXIT chart to provide insight into the proposed iterative scheme. It sheds lights on the system's error correction performance by predicting the channel signal-to-noise ratio (SNR) threshold over which the interleaved Hermitian coded system's BER starts to fall. We call the SNR threshold the pinch-off SNR limit and denote it as SNR_{off} .

Let $\mathcal{I}_a^{(\text{DET})}$ and $\mathcal{I}_e^{(\text{DET})}$ denote the mutual information of the *a priori* probabilities and the extrinsic probabilities of the MAP detector, respectively. Similarly, $\mathcal{I}_a^{(\text{DEC})}$ and $\mathcal{I}_e^{(\text{DEC})}$ denote the mutual information of the *a priori* probabilities and the extrinsic probabilities of the ABP-KV decoder. Since the decoder can feedback both the extrinsic and the deterministic probabilities, in calculating $\mathcal{I}_e^{(\text{DEC})}$, the feedback of Λ Hermitian decoding outcomes are taken as a common entity without distinguishing the probability feature. That implies

$$\mathcal{I}_e^{(\text{DEC})} = \frac{1}{\Lambda n\zeta} \sum_{t=1}^{\Lambda n\zeta} \mathcal{H}_b(P^{(\text{DEC})}(c_t)), \quad (24)$$

where $P^{(\text{DEC})}(c_t) = \tilde{P}(c_t)$ if bit c_t is decoded, or $P^{(\text{DEC})}(c_t) = P_e^{(ABP)}(c_t)$ otherwise. $\mathcal{H}_b(P^{(\text{DEC})}(c_t))$ is the binary entropy function that is defined as

$$\mathcal{H}_b(P^{(\text{DEC})}(c_t)) = - \sum_{c_t \in \{0,1\}} P^{(\text{DEC})}(c_t) \log_2 P^{(\text{DEC})}(c_t). \quad (25)$$

Let $\mathcal{T}^{(\text{DET})}$ and $\mathcal{T}^{(\text{DEC})}$ denote the extrinsic-*a priori* transfer functions of the MAP detector and the ABP-KV decoder, respectively. By realizing the MAP detector as the inner signal processing block that takes the channel observations, the EXIT curve of the MAP detector shows

$$\mathcal{I}_e^{(\text{DET})} = \mathcal{T}^{(\text{DET})}(\mathcal{I}_a^{(\text{DET})}, \text{SNR}). \quad (26)$$

Similarly, the EXIT curve of the ABP-KV decoder shows

$$\mathcal{I}_e^{(\text{DEC})} = \mathcal{T}^{(\text{DEC})}(\mathcal{I}_a^{(\text{DEC})}). \quad (27)$$

During iterations, mappings of (9) and (22) enable $\mathcal{I}_a^{(\text{DEC})} = \mathcal{I}_e^{(\text{DET})}$ and $\mathcal{I}_a^{(\text{DET})} = \mathcal{I}_e^{(\text{DEC})}$. Hence, by plotting the EXIT curve of the MAP detector and the inverted EXIT curve of the ABP-KV decoder, the interplay between the detector and decoder can be realized. In particular, a tunnel should exist between the two curves such that the iterative system is functioning with a tendency of delivering a zero bit error probability. The SNR value that just yields an exit tunnel between the two curves is the pinch-off SNR limit.

Fig.3 shows the EXIT chart of the interleaved Hermitian coded systems over PR channel I. The depth of the block interleaver is $\Lambda = 10$. The ABP decoding is functioning with $N_2 = 2$ and $N_3 = 2$, and KV decoding is functioning with $l = 10$. It can be observed that ABP-KV decoding of the interleaved (64, 39) Hermitian code yields a better extrinsic-*a priori* transfer characteristics. This is due to the fact that with the same decoding approach, the low rate code has a better error correction capability. It results in more deterministic probabilities being produced within an iteration. Consequently, the iterative system yields a lower SNR_{off} value, i.e., 5.1dB for the interleaved (64, 39) Hermitian code. While for the interleaved (64, 47) Hermitian code, $\text{SNR}_{\text{off}} = 5.4\text{dB}$.

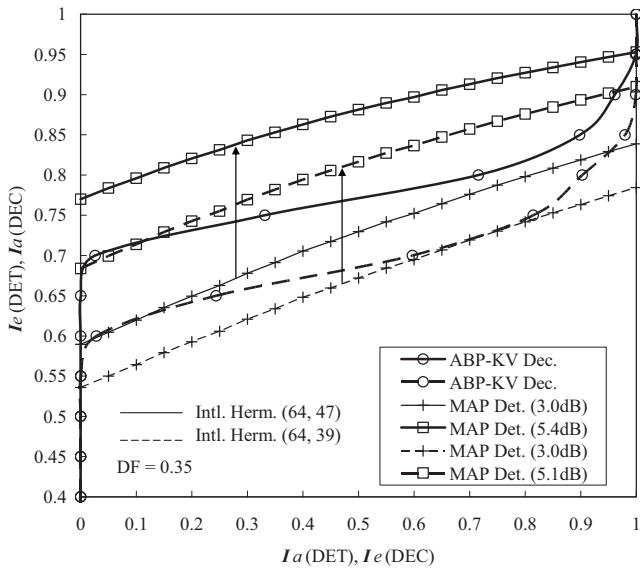


Fig. 3. Exit analysis of iterative detection-decoding of interleaved Hermitian codes over PR channel I.

TABLE I
INTERLEAVED (64, 39) HERMITIAN CODE OVER PR CHANNEL I AT 7dB

Λ	1	5	10	15
BER	1.31×10^{-3}	3.73×10^{-5}	1.25×10^{-5}	3.78×10^{-5}

Therefore, the BER curves of iterative detecting-decoding of the two interleaved Hermitian codes are predicted to fall at 5.1dB and 5.4dB, respectively. Such a prediction will be validated by simulations in the following section.

V. PERFORMANCE ANALYSIS

This section analyzes the BER performance of the proposed iterative detection-decoding of interleaved Hermitian codes on the PR channels. Let us recall N_1 , N_2 and N_3 are the designed number of global iteration, ABP iteration and BP iteration, respectively, and l is the designed factorization output list size of KV decoding. In the simulation, the ABP decoding is functioning with $N_2 = 2$ and $N_3 = 2$. Unless otherwise stated, KV decoding is functioning with $l = 10$. There are many possibilities for (N_2, N_3) , but the above setup yields the best BER performance after a heuristic search. The indicated damping factor is chosen heuristically to optimize the decoding performance. Our comparison benchmarks include Sakata's algorithm and the ABP-KV algorithm, both of which use the MAP detection but without iterative detection-decoding.

The block interleaver depth is $\Lambda = 10$ which is of sufficient size to benefit the iterative signal recovering scheme. This

TABLE II
INTERLEAVED (64, 47) HERMITIAN CODE OVER PR CHANNEL II AT 8dB

Λ	1	5	10	15
BER	4.76×10^{-3}	8.04×10^{-5}	6.04×10^{-5}	5.07×10^{-5}

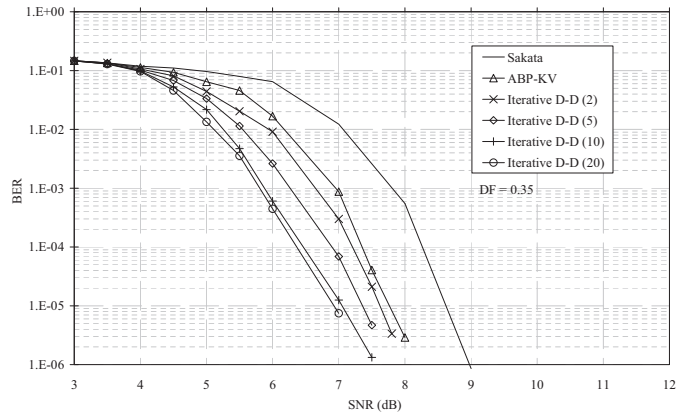


Fig. 4. Performance of the interleaved (64, 39) Hermitian code on PR channel I.

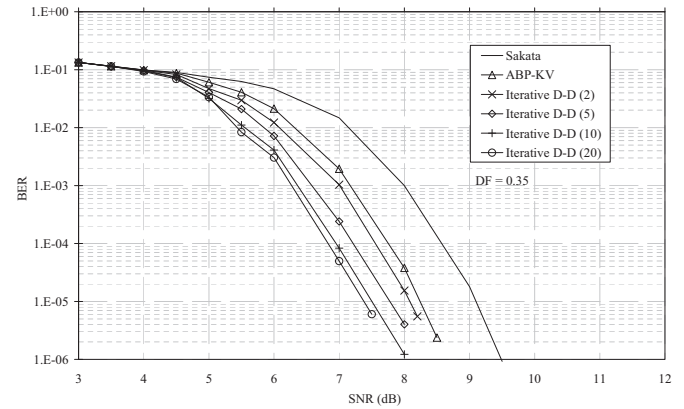


Fig. 5. Performance of the interleaved (64, 47) Hermitian code on PR channel I.

is demonstrated in Tables I and II which show the iterative detection-decoding performance of two interleaved Hermitian codes over the PR channels with $N_1 = 10$. Considering the performance-complexity tradeoff, 10 is an appropriate choice of the interleaver depth on the PR channels. It has been observed that over both of the PR channels, the output of the MAP detector contains many short burst errors of around 6 bits and individual bit errors. However, it is still necessary to have a sufficiently large block interleaver to maximize the iterative detection-decoding performance. With a larger block interleaver, more Hermitian decoding events take place within a global iteration and it is likely that more deterministic probabilities can be fed back for the MAP detection. The deterministic probabilities are beneficial for the global iteration as it improves the next round of MAP detection by considering more Hermitian codewords to be decoded later.

An alternative decoding approach for interleaved codes is the collaborative decoding [22], which can almost double the number of burst errors that can be decoded. However, the approach treats a single bit error as it does an burst error, implying it is unsuited for the channels exhibiting both burst and many bit errors. As mentioned, we have observed that the output of MAP detection over both PR channels behave like this.

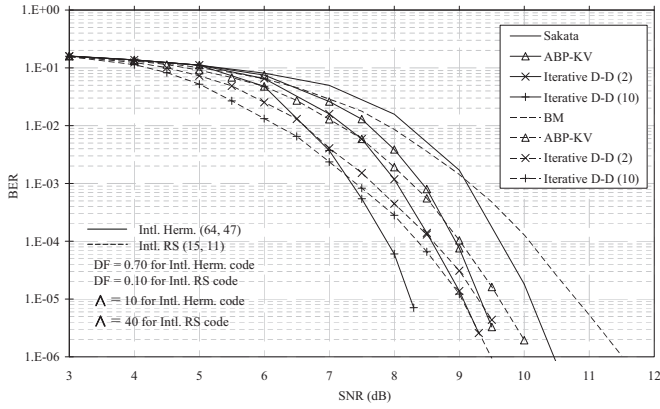


Fig. 6. Performance of the interleaved (64, 47) Hermitian code on PR channel II.

Figs.4 and 5 show the performance of the interleaved (64, 39) and (64, 47) Hermitian codes on PR channel I, respectively. They show significant coding gains can be achieved over the benchmark schemes. For the interleaved (64, 47) Hermitian code, the iterative scheme with 2 to 20 global iterations allows the code to achieve 1dB to 1.8dB coding gain at the BER of 10^{-5} over Sakata's algorithm. It demonstrates the merits of the turbo-like detection-decoding scheme for interleaved Hermitian codes. The presented results also validate the ExIT chart analysis of Section IV by showing the BER curves start to fall at the predicted SNR_{off} values.

Fig.6 compares the performance of the interleaved (64, 47) Hermitian code with the interleaved (15, 11) RS code on PR channel II which has a more severe level of ISI. Both of the codes are defined in \mathbb{F}_{16} and have a similar code rate. To ensure a fair comparison, the depth of the block interleaver for the interleaved RS code is set to $\Lambda = 40$ so that both of the interleaved codes have a similar length. It can be seen that BER performance of the interleaved Hermitian code achieves a greater error probability decay rate, resulting in a significant performance gain over the interleaved RS code. This is due to the longer Hermitian code having a larger minimum Hamming distance, and consequently inherits a greater error correction capability. Moreover, by comparing the result of Fig.5, it can be realized that as the severity of channel ISI increases, the proposed scheme achieves a greater coding gain over the non-iterative benchmark schemes.

In order to validate the performance improvement approaches mentioned in Section III.E, Fig.7 shows the performance of the interleaved (64, 47) Hermitian code on PR channel I by strengthening the ABP and KV decodings. Let N_{Θ} denote the number of attempts in restructuring the unreliable bit indices group Θ , spinning out N_{Θ} independent ABP-KV decodings. It shows that increasing N_{Θ} to 5 yields a similar performance as increasing l to 20. However, by increasing N_{Θ} to 10, it outperforms the KV decoder-strengthening approach. However, those performance improvement approaches tend to play a less significant role than setting a greater global iteration number N_1 . Considering they are at the expense of system complexity, moderate ABP-KV decoding parameters

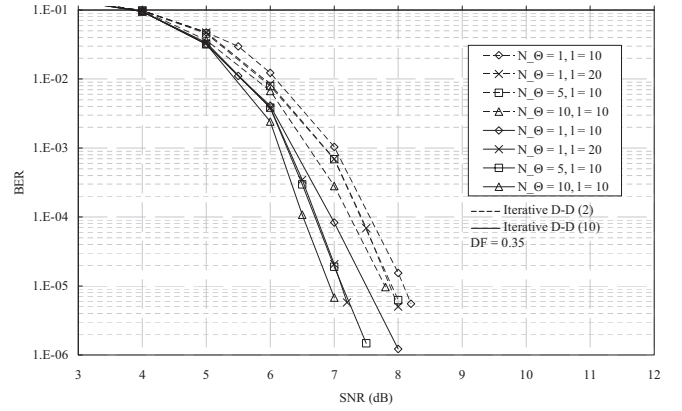


Fig. 7. Improved performance of the interleaved (64, 47) Hermitian code on PR channel I.

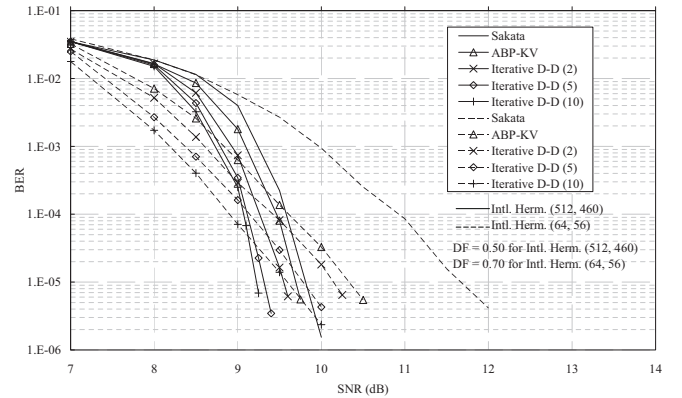


Fig. 8. Performance of the interleaved (512, 460) Hermitian code on PR channel II.

are recommended, as exemplified by our simulation setup.

Finally, Fig.8 shows the performance of the interleaved (512, 460) Hermitian code defined in \mathbb{F}_{64} on PR channel II. In order to show the advantage of using a long code, its performance is compared with the interleaved (64, 56) Hermitian code with a similar code rate. Due to the large amount of short cycles in matrix \mathbf{H}'_b of the long code, its ABP decoding utilizes the Min-Sum extrinsic LLR calculation in (16). It shows the long code outperforms the short code with a more significant performance advantage in the deep BER region. Again, this thanks to the long code having a larger minimum Hamming distance. However, notice that iterative decoding of the long code does not achieve as large coding gains over the Sakata and ABP-KV schemes. There are two reasons for this: First, the adapted matrix \mathbf{H}'_b of the long code has a much larger number of short cycles than the short code. Consequently, the ABP algorithm is not as capable in enhancing the soft received information as it for the short code. Second, both codes use a block interleaver of depth 10 and it may not be an ideal size for the long code. However, using a larger interleaver depth for the long code would make the comparison less fair.

VI. COMPLEXITY ANALYSIS

The proposed iterative scheme requires three types of arithmetic computations: floating point, binary and finite field. We now analyze the computational cost of a global iteration. Letting Ω^2 denote the number of trellis states in the MAP detector, the MAP detection requires $O(\Omega\Lambda n\zeta)$ floating point operations. In decoding a Hermitian code, each BP iteration requires $O((n\zeta)^3)$ floating point operations. Hence, the BP decoding dominates the floating point operation. Considering N_3 BP iterations will be performed in each of the N_2 ABP iterations, a global iteration requires at most $O(N_2N_3\Lambda(n\zeta)^3)$ floating point operations. Each Gaussian elimination requires $O((n\zeta)^3)$ binary operations, and hence a global iteration requires at most $O(N_2\Lambda(n\zeta)^3)$ binary operations. Finally, KV decoding requires $O(n^2l^5)$ finite field operations [8] [23]. Note that [23]'s conclusion on KV decoding complexity for RS codes also holds for Hermitian codes. Considering it is performed for each adapted matrix \mathbf{H}'_b , a global iteration requires at most $O(N_2\Lambda n^2l^5)$ finite field operations. In practice, the decoding latency will be dominated by the KV decoding as it requires the more complex finite field operation. However, for long Hermitian codes, e.g., the (512, 460) Hermitian code, the Gaussian elimination and BP decoding will also take a larger portion of the latency as they deal with a large parity-check matrix with a relatively high density.

It is important to point out that the above analysis defines the maximal complexity of a global iteration. Decoding of the interleaved code is performed in a successive cancellation manner meaning that the decoded Hermitian codeword will not be decoded again in any of the following iterations. Therefore, as the global iteration progresses, the number of KV decoding events will be reduced. With a mildly corrupted received information, it is likely that all the codewords are decoded before the final iteration, so the actual computation complexity is channel dependent. The decoding latency can be reduced by parallelizing all the Λ outer decoding events. It will be interesting to investigate the consequences of replacing the sophisticated KV decoding with the simpler and less computationally intensive Sakata minimum-distance decoding. Studies have indicated that the performance loss could be relatively minor [10].

VII. CONCLUSION

This paper has proposed an iterative soft detection-decoding scheme for interleaved Hermitian codes that can be employed on magnetic storage channels that exhibit a combination of burst errors and individual bit errors. The proposed scheme integrates the MAP detection and the ABP-KV decoding, enabling the extrinsic probabilities of the Hermitian coded bits to be iterated between the two soft-decision processes. In order to improve the iterative detection-decoding performance, two ABP-KV decoding performance improvement approaches have been introduced. The ExIT chart analysis of the proposed scheme on the PR channel has been presented, showing the interplay between the soft detector and the soft decoder and

highlighting the error correction performance of the proposed scheme. Our performance analysis has shown that significant coding gains can be achieved over conventional schemes that treat the detection and decoding as two separate processes. More importantly, we have also shown the performance advantage of interleaved Hermitian codes over interleaved RS codes, demonstrating the benefit of employing Hermitian codes for high density storage devices. Finally, the computational complexity of the proposed scheme has been analyzed with proposal on more efficient implementation of the iterative scheme.

REFERENCES

- [1] V. D. Goppa, "Codes on algebraic curves," *Soviet Math*, vol. 24, pp. 75–91, 1981.
- [2] M. Johnston and R. A. Carrasco, "Construction and performance of algebraic-geometric codes over awgn and fading channels," *IEE Proc. Commun.*, vol. 152, pp. 713–722, 2005.
- [3] S. Sakata, J. Justesen, Y. Madelung, H. E. Jensen, and T. Hoholdt, "Fast decoding of algebraic-geometric codes up to the designed minimum distance," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1672–1677, Nov. 1995.
- [4] V. Guruswami and M. Sudan, "Improved decoding of reed-solomon and algebraic-geometric codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1757–1767, Sep. 1999.
- [5] T. Hoholdt and R. R. Nielsen, "Decoding hermitian codes with sudan's algorithm," *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Lecture Notes in Computer Science)*, pp. 260–270, 1999.
- [6] L. Chen, R. A. Carrasco, and M. Johnston, "Reduced complexity for list decoding hermitian codes," *IEEE Trans. Wirel. Commun.*, vol. 7, no. 11, pp. 4353–4361, Nov. 2008.
- [7] R. Koetter and A. Vardy, "Algebraic soft-decision decoding of reed-solomon codes," *IEEE Trans. Inform. Theory*, vol. 49, no. 11, pp. 2809–2825, Nov. 2003.
- [8] L. Chen, R. A. Carrasco, and M. Johnston, "Soft-decision list decoding of hermitian codes," *IEEE Trans. Commun.*, vol. 57, no. 8, pp. 2169–2176, Aug. 2009.
- [9] K. Lee and M. E. O'Sullivan, "Algebraic soft-decision decoding of hermitian codes," *IEEE Trans. Inform. Theory*, vol. 56, no. 6, pp. 2587–2600, Jun. 2010.
- [10] L. Chen, "Iterative soft-decision decoding of hermitian codes," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 33–42, Jan. 2013.
- [11] M. Fossorier and S. Lin, "Soft-decision decoding of linear block codes based on ordered statistics," *IEEE Trans. Inform. Theory*, vol. 41, no. 5, pp. 1379–1396, Sep. 1995.
- [12] L. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," *IEEE Trans. Inform. Theory*, vol. 20, pp. 284–287, Mar. 1974.
- [13] H. Song, R. M. Todd, and J. R. Cruz, "Low density parity check codes for magnetic recording channels," *IEEE Trans. Magn.*, vol. 36, no. 5, pp. 2183–2186, Sep. 2000.
- [14] B. M. Kurkoski, P. H. Siegel, and J. K. Wolf, "Joint message-passing decoding of ldpc codes and partial-response channels," *IEEE Trans. Inform. Theory*, vol. 48, no. 6, pp. 1410–1422, Jun. 2002.
- [15] S. ten Brink, "Convergence behavior of iteratively decoded parallel concatenated codes," *IEEE Trans. Commun.*, vol. 49, no. 10, pp. 1727–1737, Oct. 2001.
- [16] R. Horn and C. Johnson, *Matrix Analysis*. Cambridge Univ. Press, 1985.
- [17] J. G. Proakis, *Partial response equalization with application to high density magnetic recording channels*. CRC Press, 2005, ch. 8, pp. 1–23.
- [18] M. Madden, M. Oberg, Z. Wu, and R. He, "Read channel for perpendicular magnetic recording," *IEEE Trans. Magn.*, vol. 40, no. 1, pp. 241–246, Jan. 2004.
- [19] J. Moon and W. Zeng, "Equalization for maximum likelihood detectors," *IEEE Trans. Magn.*, vol. 31, no. 2, pp. 1083–1088, Mar. 1995.
- [20] X. W. Wu and P. Siegel, "Efficient root-finding algorithm with application to list decoding of algebraic-geometric codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 6, pp. 2579–2587, Sept. 2001.

²In PR channel I $\Omega = 4$, and in PR channel II $\Omega = 8$.

- [21] L. Chen, R. A. Carrasco, M. Johnston, and E. G. Chester, "Efficient factorisation algorithm for list decoding algebraic-geometric and reed-solomon codes," *Proc. IEEE Int. Conf. Commun.(ICC)*, May 2007.
- [22] S. Kampf, "Bounds on collaborative decoding of interleaved hermitian codes and virtual extension," *Designs, Codes and Crypto.*, vol. 70, pp. 9–25, 2014.
- [23] L. Chen, S. Tang, and X. Ma, "Progressive algebraic soft-decision decoding of reed-solomon codes," *IEEE Trans. Commun.*, vol. 61, no. 2, pp. 433–442, Feb. 2013.