Optimizing the Co-Design of Message Structure and Channel Coding to Reduce the TTD for a Galileo 2nd Generation Signal

Lorenzo Ortega, Charly Poulliat, Marie-Laure Boucheret, Marion Aubault-Roudier, Hanaa Al Bitar-El Natour

Optimizing the co-design of message structure and channel coding to reduce the TTD for a Galileo 2nd generation signal

Lorenzo Ortega[1,2] ⓘ   **Charly Poulliat**[2] ⓘ   **Marie Laure Boucheret**[2] ⓘ

Marion Aubault-Roudier[3] | **Hanaa Al-Bitar**[4]

[1] TeSA, Toulouse, France

[2] University of Toulouse, Toulouse, France

[3] CNES, Toulouse, France

[4] Thales Alenia Space, Toulouse, France

Correspondence
Lorenzo Ortega Espluga, TeSA, Toulouse, France.
Email: lorenzo.ortega@tesa.prd.fr

Abstract

Recently, the joint design of the GNSS message structure and the associated channel-coding scheme have been investigated as a means to reduce the Time-To-First-Fix (TTFF) and particularly the time to retrieve the Clock and Ephemerides Data (CED). In this context, a new method to co-design the navigation message and the channel-coding scheme structure is proposed in this paper. This new co-design enables us to reduce the time to retrieve the CED while enhancing error-correction capabilities under degraded channel conditions. In order to fulfill such requirements, some structured coding schemes are designed, which provide both maximum distance separable (MDS) and full diversity properties under a non-ergodic channel assumption.

1   INTRODUCTION

Recently, the interest for reducing the Time-To-First-Fix (TTFF) in GNSS systems has motivated some research on new channel-coding schemes enabling the decrease of the time to retrieve the Clock and Ephemerides Data (CED), also called Time-To-Data (TTD) (Schotsch, Anghileri, Burger, and Ouedraogo 2017). Such coding schemes exploit both serial concatenation and the Maximum Distance Separable (MDS) property in order to retrieve reliably the information data as fast as possible. From Schotsch et al. (2017) and Ortega Espluga, Poulliat, Boucheret, Aubault, and Al Bitar (2018b), it has also been observed that those current channel-coding designs may, however, not perform sufficiently well in terms of error-correction capability, and as a consequence, the resilience of the data can be degraded under harsh environments.

In this paper, we provide a new methodology to design jointly the navigation message structure and the channel-coding scheme. The proposed method is able to reduce the TTD and to provide enhanced error-correction capabilities under low Carrier-to-Noise ratio (C/N_0) environments.

Moreover, concerning the channel-coding part, the proposed method combines error-correcting techniques with error-detecting techniques in order to ensure the robustness of the CED, as it has been already the case in Schotsch et al. (2017) and Ortega Espluga et al. (2018b).

In order to be able to design some new suitable error-correcting schemes, taking into account the message structure, we start by modeling the navigation message acquisition and detection as a specific non-ergodic channel (Biglieri, Proakis, & Shamai, 1998), commonly referred to as a block-fading channel and which can be seen as an extension of the already presented erasure-channel model (Ortega Espluga et al., 2018b). For this channel, the message and the redundant bits from the channel encoder are divided into different encoded information blocks. Each block may experience different channel conditions, resulting in blocks that are each weighted by a different fading coefficient (large-scale variations). In case of a deep fade, the receiver assumes that no data has been transmitted and an erasure-channel assumption can be done.

In our context, the received signal model can be modeled as a block-fading channel with block erasures, which means that:

- Some information blocks are received with errors and different average signal-to-noise ratios;
- Some information blocks are missing.

Co-designing the message and channel coding under the block-fading channel with the block-erasure assumption helps us to describe how the CED can be retrieved in spite of missing data (labelled as erased data) and also to describe the method to reduce the TTD.

Moreover, such a model enables us to provide the requirements to obtain the two desired channel-coding properties, i.e., the MDS and the full diversity properties. The MDS property allows us to retrieve k data units of systematic information from any k error-free data units of information (no matter whether it is systematic or redundant information). It must be noted that, in this case, the information symbols correspond to the block defined by the message structure design. On the other side, the full diversity property allows us to create an error-correction code structure to attenuate the degradation in rough environments.

In this paper, capitalizing on some of our preliminary proposals (Ortega Espluga, Poulliat, Boucheret, Aubault, & Al Bitar, 2018a), we investigate error-correcting schemes, which seek the desired properties (i.e., MDS and full diversity). The four different schemes that will be studied are as follows:

1. The first scheme is based on the use of the Lowest Density Maximum Distance Separable (LD-MDS) codes (Blaum & Roth, 1999) of coding rate $R = 1/2$ using a message-passing decoding algorithm based on Belief Propagation (BP) in conjunction with a low-complexity erasure algorithm at the decoding part.
2. The second error-correcting technique proposes to use a sparse MDS code (also of coding rate $R = 1/2$), instead of a LD-MDS code, in order to improve the poor error-correcting performance achieved by the LD-MDS codes, since those channel codes are mainly designed for channels with erasures.
3. The third scheme proposes a new family of structured codes called regular Root-LDPC codes (Boutros, Fàbregas, Biglieri, & Zémor, 2010) of coding rate $R = 1/2$. It is shown that such an error-correcting code family can have both the MDS and the full diversity properties under the BP decoding algorithm, as long as the CED and redundant data are divided into two information blocks. Thanks to this property, both the error-correction and erasure-correction capabilities are achieved just by running the soft input BP decoding algorithm. To take into account channel variations smaller than an information block, two independent block interleavers are also used to average the channel over each information block.
4. The last scheme extends the previous scheme to irregular Protograph Root-LDPC codes of rate $1/2$. This family breaks the regular structure defined in the previous scheme in order to optimize the error-correction capabilities (i.e., the convergence/demodulation threshold) under the BP decoding algorithm. Designing theses codes is possible thanks to tools such as density evolution (Ryan & Lin, 2009) or the Protograph EXIT-Chart Algorithm (Liva & Chiani, 2007). In this paper, the latter method has been used in order to design good protograph codes. As in the preceding case, two independent block interleavers are also added to average the channel over each information block.

The four error-correcting schemes along with a new message structure are simulated and compared to each other. The proposed schemes are also compared to the GPS L1C CED error-correcting scheme (IS-GPS-800, 2018), that will be considered as a benchmark system, the Galileo E1B I/NAV message (OS SIS ICD, 2016) and the RS2 configuration of the Galileo E1B I/NAV message (Schotsch et al., 2017), proposed to improve the CED robustness as well as to reduce the TTD. Simulations are performed for the additive white Gaussian noise (AWGN) channel and for an urban scenario modeled through the two-state Prieto model (Prieto-Cerdeira, Perez-Fontan, Burzigotti, Bolea-Alamañac, & Sanchez-Lago, 2010).

The paper is organized as follows. Section 2 presents the requirements for co-designing the message structure and the channel coding to reduce the time to retrieve the CED. In Section 3, an introduction to the block-fading-channel model as well as the desired coding properties in such an environment are provided. Section 4 reviews the current GPS L1C structure since it is considered as the benchmark regarding the time needed to retrieve the CED and the current structure of the Galileo E1B I/NAV message as well as the RS2 configuration. Section 5 presents the error-correcting solutions. Their performance are presented and analyzed over the block-fading channel in Section 6. Then, we present the performance over standard channels like AWGN or urban channels in Section 7. Conclusions are finally drawn in Section 8.

2 | CO-DESIGN OF MESSAGE OF STRUCTURE AND CHANNEL CODING

One of the most challenging issues to provide the lowest *TTFF* is to design fast acquisition GNSS signals. *TTFF* is defined as the time needed by the receiver to calculate the first position fix and can be considered as a
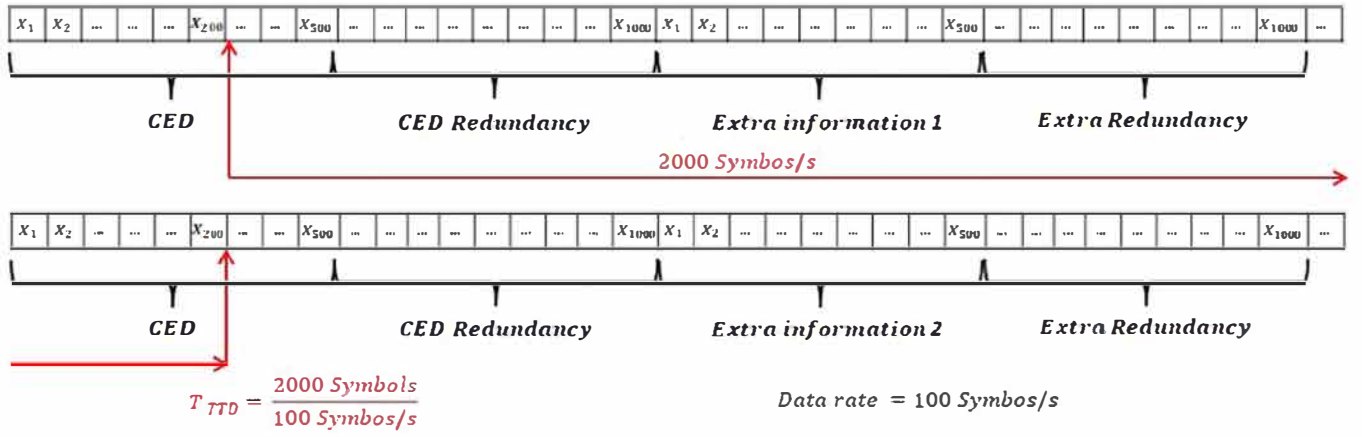
FIGURE 1 Navigation message structure [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

contribution of different times, including the time to retrieve the CED data, denoted TTD, and which represents the major contribution of the *TTFF* (Schotsch et al., 2017). In this paper, we provide a new data-navigation-message acquisition model, which allows us to design suitable error-correcting schemes to reduce the TTD. Thanks to this new model, we aim to manage a reduction of the time to retrieve the CED under high C/N_0 environments without degrading the performance under low C/N_0 channel conditions.

Assuming a GNSS receiver under a cold start scenario (no data is stored in the receiver), the GNSS receiver can start to acquire the information data in any symbol period of the navigation message. If that symbol corresponds to the first information bit of the CED, the optimal TTD is obtained, otherwise all the navigation messages must be received in order to decode the CED (which implies the highest TTD). This situation is illustrated in Figure 1, where the first acquired symbol is marked with the red arrow resulting in the fact that the complete navigation message must be received in order to decode the CED.

Considering the preceding idea, we propose in this article a new data-navigation acquisition model, which proposes to describe the navigation message as a block-fading channel with erasure block. Thanks to this assumption, we can model:

- The missing navigation data (not yet received) as an erased block.
- The received navigation data as recovered information with different average signal-to-noise ratios.

The idea to model the data navigation acquisition as a block-fading channel with block erasures is to find navigation message structures for which the CED can be decoded even if some part of the message has not been received yet. In that case, the TTD can be reduced since the receiver does not need to receive all the navigation data to decode the CED.

Considering the data-navigation acquisition model, and in order to reduce TTD, we propose in this paper a method to design jointly the message structure and the channel coding. This co-design fulfills the following requirements:

1. CED and redundant data (from the channel coding) are divided in several blocks. At the receiver, if any block has not been received, the decoder must consider that block as an erased block.
2. A Cyclic redundancy check (CRC) code is used to append error-detection data that must be included within the CED. This CRC code is used to check the integrity of the CED.
3. The co-design must provide the capability to decode the CED even if some information blocks are missing/erased. However, we have to emphasize the fact that missing information blocks limit the error-correcting capabilities. Therefore, if the CRC detects an error, the receiver can still wait for missing erased blocks in order to enhance the error-correcting capabilities. This is crucial in order to be able to retrieve the CED under harsh environments.
4. If we assume that the CED and redundant data are part of a codeword, a co-design scheme does not allow the use of entire codeword interleavers (as it is done in classical systems). Indeed, this structure enforces us to receive the *entire* codeword to decode the CED. Consequently, considering a co-design scheme with an interleaver spanning the entire codeword cannot help to reduce the TTD compared to existing systems.
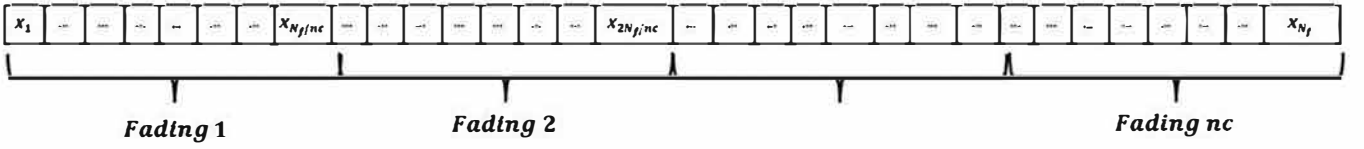
FIGURE 2 Message structure

3 | BLOCK-FADING CHANNEL AND DESIRED CODING PROPERTIES

3.1 | Block-fading-channel model

The non-ergodic block-fading channel (Boutros et al., 2010) is a simplified channel model that characterizes slowly varying fading channels. It can be viewed as an extension of the well-known block-erasure channel, which considers that some parts of the message are completely erased due to a deep fade of the channel or because of the lack of received data. Indeed, the block-erasure channel corresponds to the specific case of the largest signal-to-noise ratio case of the block-fading channel, where some parts of the codewords are received with a high signal-to-noise ratio (SNR) and the other parts are received with a lower SNR. Under this context of a non-ergodic channel, a transmitted codeword can be viewed as a finite number n_c of independent channel realizations.

We consider a block-fading channel with n_c fading blocks, whose discrete-time channel output at time i is given by:

$$y_i = h_i x_i + z_i, i = 1, \ldots, N_f, \tag{1}$$

where N_f denotes the frame length, $x_i \in \{-1, +1\}$ is the $i - th$ binary phase shift keying (BPSK) modulated symbol, $z_i \sim \mathcal{N}(0, \sigma^2)$ are the centered i.i.d. Gaussian noise samples with variance $\sigma^2 = N_0/2$, and h_i is a real fading coefficient that belongs to the set $\mathbb{N} = \{\alpha_1, \alpha_2, \ldots, \alpha_{nc}\}$. Figure 2 illustrates a codeword under the block-fading-channel scenario.

Similarly to any other non-ergodic channel, the block-fading channel has zero capacity in the strict Shannon sense. To assess performance under this scenario, the information outage probability, which is an implicit function of the average SNR γ, is usually defined as follows:

$$P_{out}(\gamma) = Prob\{I_\mathbb{N} \leq R\}, \tag{2}$$

where $I_\mathbb{N}$ denotes the instantaneous mutual information between the BPSK constrained input and the noisy observation at the output of the channel for a particular channel realization $\mathbb{N}$, and R is the transmission rate in bits per
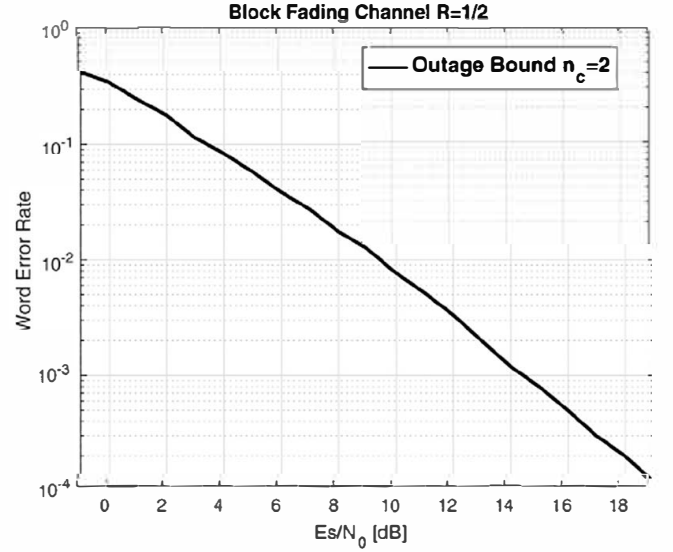

FIGURE 3 Outage probability P_{out} for a BPSK input with $R = 1/2$, represents the ideal code for a block-fading channel $n_c = 2$ (black/solid line)

channel use. Then, $I_\mathbb{N}$ can be calculated as:

$$I_\mathbb{N} \triangleq \frac{1}{n_c} \sum_{i=1}^{n_c} I_{AWGN}(\gamma \alpha_i^2), \tag{3}$$

where $I_{AWGN}(s)$ is the input-output mutual information for a binary input AWGN channel with a SNR equal to s ($I_{AWGN}(s)$ is also referred to as the constrained input AWGN capacity for BPSK inputs) and $\alpha_i, i \in (1, \ldots n_c)$, are the instantaneous fading gains for each block i. These fading gains follow a normalized Rayleigh distribution in the case of the block Rayleigh fading channel. In such a non-ergodic channel, P_{out} gives a lower bound on the codeword error probability. In Figure 3, P_{out} is illustrated for a BPSK input with $R = 1/2$, which represents the ideal behavior of a code for a block-fading channel with $n_c = 2$.

3.2 | Desired code properties

In order to design codes suited for the non-ergodic channels, two main properties are required:

1. MDS (Maximum Distance Separable property),
2. Full Diversity.

Let us consider a channel-coding scheme, which provides codewords divided in n blocks of equal sizes. We further assume that the systematic information is embedded into k blocks with $k < n$ of the same size. The MDS property allows us to retrieve k data blocks of systematic information from any k error-free received blocks. In other words, thanks to this property we can reduce the time to retrieve CED under high C/N_0 environments, since with only k error-free data blocks, the CED can be retrieved. On the other hand, several references (Boutros et al., 2010; Fabregas & Caire, 2006; Knopp & Humblet, 2000) exhibit the poor error-correction performance over non-ergodic channels, which are not able to achieve a good *coding gain*. In order to achieve better error-correction capabilities, the *full diversity* property is further required.

Definition 1. An error-correcting code is C said to have full diversity over the block-fading channel if the diversity order is equal to the number of fading blocks n_c. The *diversity* order determines the slope of the error-rate curve as a function of the SNR on a log-log scale for Rayleigh fading distribution:

$$d = - \lim_{\gamma \to \infty} \left(\frac{\log(P_{ew}(\gamma))}{\log(\gamma)} \right), \qquad (4)$$

where P_{ew} is the codeword error probability at the decoder output and γ is the average SNR. Then, the P_{ew} of a code with full diversity n_c decreases as $1/\gamma^{n_c}$ at high SNR. Since the error probability of any coding/decoding scheme is lower-bounded by the outage probability P_{out}, the diversity order is upper-bounded by the intrinsic diversity of the channel, which reflects the slope of the outage limit. In other words, when the coding/decoding scheme has the same slope as for the outage probability curve, then the coding scheme is referred to as *full diversity* for the aforementioned block-fading channel. Given a codeword $x \in C$ from the error-correcting code, we define the blockwise Hamming weight $(w_1(x), w_2(x), \ldots, w_{nc}(x))$, where $w_j(x)$ is the Hamming weight of coded bits affected by fading h_j. Then, under the maximum likelihood of decoding, the diversity order can also be determined by Fabregas and Caire (2006)

$$d = \min_{x \in C - 0} |\{w_j(x) \neq 0\}|. \qquad (5)$$

In other words, d is the minimum number of blocks that have nonzero Hamming weight. We refer to it as the block-wise minimum Hamming distance.

When maximum diversity is achieved by a code, the coding gain yields a measure of "SNR proximity" to the outage limit. This optimal design yields the optimal code, which is given by the Singleton bound:

$$d \leq 1 + \lfloor n_c (1 - R) \rfloor. \qquad (6)$$

Note that d is referred to as the code block diversity and is given by the minimum number of blocks on which any two distinct codewords differ (i.e., the block-wise Hamming distance).

Codes achieving the Singleton bound are termed MDS. MDS codes are outage-achieving over the (noiseless) block-erasure channel, but may not achieve the outage probability limit on noisy block-fading channels and, as a consequence, a good coding gain. As a matter of fact, MDS codes are necessary, but not sufficient to approach the outage probability of the channel. Thus, for noisy channels, we aim to design error-correcting schemes that ensure the full diversity property (P_{cm} is asymptotically parallel to the outage bound) and to try to operate as close as possible to the outage bound (good coding gain). Notice from Equation (6) that, in order to find a full diversity code ($d = n_c$), the maximum achievable rate is $R = 1/n_c$.

4 | REVIEW OF SOME EXISTING MESSAGE STRUCTURES

4.1 | GPS L1C channel-coding scheme and message structure

In this section, we briefly review how the CED information is encoded for GPS L1C (Roudier, 2015).

The message modulated onto the GPS L1C signal consists of a set of consecutive frames, where the complete data message set is broadcasted to users. A frame is divided into three subframes of various lengths. The first subframe consists of 9 bits of Time of Interval (TOI) data. The subframe 2 is composed of 600 bits of non-variable clock and ephemeris data with Cyclic Redundancy Check (CRC). The content of subframe 3 nominally varies from one frame to the next and is identified by a page number; the size of the block is 250 bits. Each of the subframes is encoded as follows:

1. The 9-bit TOI data of subframe 1 are encoded with a BCH code;
2. Subframe 2 data are encoded using a 24-bit CRC code and an irregular Low-Density Parity-Check (LDPC) Forward Error-Correction (FEC) code using a parity check matrix of size 600×1200;
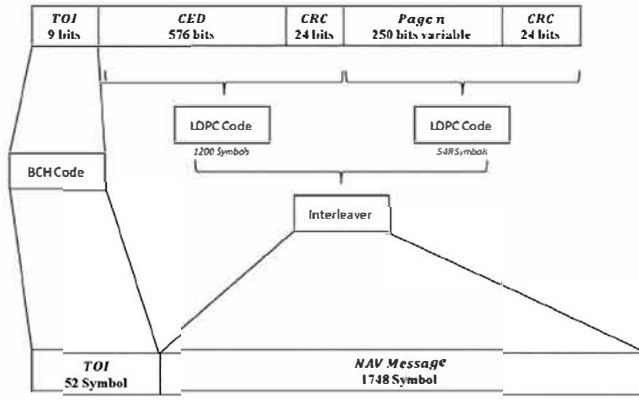3. Subframe 3 data are encoded using a 24-bit CRC code and an irregular Low Density Parity Check (LDPC)

FIGURE 4 GPS L1C message structure

FIGURE 5 I/NAV $S_{E1-OS_{data}}$ nominal subframe layout (Baseline and RS2 configuration) [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

Forward Error-Correction (FEC) code with a parity check matrix of size 274 × 548;

4. Encoded data from subframe 2 and 3 are then interleaved. The resulting 1,800 symbols represent one message frame, which are then broadcast at a rate of 100 symbols per second. Figure 4 gives the structure of the described GPS L1C message.

Nowadays, the GPS L1C navigation message provides a structure which allows us to decode the CED in the shortest time when compared with other navigation message structures. For example, the worst-case TTD is of the order of 18s, which has to be compared to the 32s of Galileo E1B I/NAV. The GPS L1C standard also uses state of the art error-correcting codes, such as the irregular LDPC code of rate 1/2 used to protect the GPS L1C structure subframe 2 (where the CED is located), which provides low demodulation threshold and outstanding error-correction capabilities. Additionally, the GPS L1C structure uses a block interleaver, which is used for the symbols allocated within the subframe 2 and subframe 3 in order to improve the performance over block-fading channels. For all these reasons, GPS L1C can be considered as a natural choice for benchmarking when we aim to design a navigation message that enables us to improve the time to retrieve the CED. It is also a practical lower bound for existing systems. The idea of our proposal is to try to keep best features among existing (and still efficient) structures while enabling modifications that can help to improve the decoding delay. This is mainly the reason why we are aiming to capitalize on the naturally efficient structure of the GPS L1C.

4.2 | Review of Galileo I/NAV message (baseline and new configurations)

Of course, there are other navigation message structures embedding error-correcting schemes in order to improve

the robustness of the CED and to reduce the TTD. However, those structures provide worse results than GPS L1C in terms of error-correction performance and TTD. Thus, as a remarkable example, we first consider the Galileo I/NAV message, used to send the data component of the Galileo E1-B signal. The structure of the I/NAV message is presented in OS SIS ICD (2016). It is composed of 15 nominal pages, each one with a duration of two seconds, giving the 30-second duration of the I/NAV subframe structure illustrated in Figure 5. Within the subframe structure, pages 1, 2, 11, and 12 are used to store the four CED information words. Therefore, every 30 seconds, four CED information words are provided by the I/NAV message. Each nominal page is subdivided into two subpages. Each subpage has 120 bits, and it is encoded by a rate of one-half convolutional code with polynomial generators in octal representation given by $(171, 133)_8$ (OS SIS ICD, 2016). At the output of the convolutional encoder, 240 data symbols are interleaved by a 30 × 8 block interleaver. Finally, 10 synchronization bits are added at the beginning of the data frame to achieve synchronization to the page boundary. At the receiver, each page is decoded independently. First, the synchronization pattern allows the receiver to achieve synchronization to the page boundary. Each page is then deinterleaved by a 8 × 30 block interleaver and decoded using the Viterbi algorithm (Viterbi, 1967) to perform maximum likelihood detection. Finally, the CRC is checked. In order to retrieve the CED, pages 1, 2, 11, and 12 must be validated using the CRC. Using this structure, it can be shown that in some cases the CED cannot be retrieved before 32 seconds. In order to overcome this drawback, some proposal (Ortega Espluga et al., 2018b; Schotsch et al., 2017) has been proposed to improve the I/NAV message. Those proposals

take advantage of the possibility to use unassigned pages within the Galileo I/NAV message. This design of the new signal seeks to reduce the TTD and to improve the CED robustness while ensuring the backward compatibility with the current I/NAV message structure. As an example, we decide to implement the RS2 configuration (Schotsch et al., 2017), where pages 6 and 7 were selected to store the redundant data generated by a Reed Solomon (RS) outer channel code. With this setting in mind, a general outer channel-coding $(n, k) = (6, 4)$ structure can be defined in order to generate those extra redundant bits, where n is equivalent to the total number of available bits (redundant + information bits) and k is the number of information bits. In order to keep backward compatibility, systematic information bits are stored in pages 1, 2, 11, and 12 while redundant bits are stored in pages 6 and 7. Remark that the RS codes are MDS codes, then CED can be decoded when a number of at least $k = 4$ pages are retrieved, which ensures a faster recovery than for the baseline I/NAV message. In Figure 5, the I/NAV $S_{E1-OS_{data}}$ nominal subframe layout (Baseline and RS2 examples) is illustrated.

5 | ERROR-CORRECTING SCHEMES

In this section, we present four proposed error-correcting schemes, which aim to capitalize on the MDS and full diversity properties previously described in Section 3. Those channel error-correcting schemes follow the parameters of the GPS L1C CED channel-coding scheme, with coding rate $R = 1/2$ and code structure $C(u, m)$ with $u = 600$ and $m = 1200$.

5.1 | Lowest density maximum distance separable (LD-MDS) codes

LD-MDS (Blaum & Roth, 1999) codes were already proposed in Ortega Espluga et al. (2018b) as a possible solution for the new Galileo I/NAV navigation coding scheme. Those codes combine two main properties. The first property is the Maximum Distance Separable (MDS) property (Blaum & Roth, 1999), which allows us to retrieve k data symbols of information from any k error-free symbols (no matter systematic or redundant information). The second property is the sparsity of the parity-check matrix. This enables the use of efficient low-complexity decoding algorithms (Blaum & Roth, 1999). It must be noted that the lowest sparsity property does not provide codes that can operate close to the outage probability region (due to the fact that they do not exhibit the full diversity property), and as a consequence, the LD-MDS are not considered as good codes under the message-passing algorithm over noisy channels, such as Belief-Propagation (BP). More-

over, since the LD-MDS codes under the BP decoding algorithm do not exhibit the MDS property, a tailored erasure-correcting algorithm must be developed in order to exploit their MDS property. For more details about LD-MDS codes, please refer to Blaum and Roth (1999).

In order to design a LD-MDS code of rate $1/2$, Blaum and Roth (1999) presents the construction of a linear $[k + 2, k]$ MDS code over $GF(q^b)$ whose systematic parity check and generator matrices are defined as follows:

$$H_\beta = \begin{bmatrix} I & I & I & \dots & I & I & 0 \\ \beta_1 & \beta_2 & \beta_3 & \dots & \beta_k & 0 & I \end{bmatrix} \quad (7)$$

$$G_\beta = \begin{bmatrix} I & 0 & 0 & \dots & 0 & -I & -\beta_1^T \\ 0 & I & 0 & \dots & 0 & -I & -\beta_2^T \\ 0 & 0 & I & \dots & 0 & -I & -\beta_3^T \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & I & -I & -\beta_k^T \end{bmatrix}, \quad (8)$$

where $\beta = \{\beta_1, \beta_2, \dots, \beta_k\}$ is a collection of $b \times b$ matrices over $GF(q)$ and I is the identity matrix. In order to build a MDS code, the collection β must follow the following properties:

- (P1) Each matrix in the set is nonsingular.
- (P2) Every two distinct matrices in the set have a difference that is also nonsingular.

Moreover, the fewer 1's in the parity check matrix, the lower complexity in the coding and decoding algorithms. As a consequence, we have the following property:

- (P3) Each matrix contains at most $b + 1$ nonzero elements.

When considering the restriction of those codes to the binary field ($q = 2$), and in order to construct a set of matrices β satisfying (P1)–(P3) (Blaum & Roth, 1999), we defined the set of matrices as $Q_\alpha^i = \{v_{l,m}\}$, where $v_{l,m}$ are defined as follows:

Definition 2. Let p as an odd prime and α as an element of $GF(q) - \{0\}$. In our case as $q = 2$, $\alpha = 1$. For $0 \leq i < p$, we define the set of matrix of dimension $b \times b = (p - 1) \times (p - 1)$ as $Q_\alpha^i = \{v_{l,m}\}$, where $l, m \in (1, p - 1)$ over $GF(q)$. Considering the parameters $q = 2$ and $\alpha = 1$, the set of matrices $Q_\alpha^i = \{v_{l,m}\}$ over $GF(2)$ are defined by:

$$v_{l,m} = \begin{cases} 1 \text{ if } l \neq p - i \text{ and } \langle m - l \rangle = i \\ 1 \text{ if } l = p - i \text{ and } m = i \\ 1 \text{ if } l = p - i \text{ and } m = \langle i/2 \rangle. \\ 0 \text{ otherwise} \end{cases} \quad (9)$$

The operator $\langle . \rangle$ denotes the *mod p* operation, and $\langle a/2 \rangle$ denotes the integer between $0 \le \sigma \le p$, such that $a \equiv b\sigma (mod\ p)$. In order to design binary MDS codes, the following theorem provides sufficient conditions on p and α so Q_α^i satisfy (P2).

Theorem 1 (Blaum & Roth, 1999). *Let p be a prime such that $p - 1$ is divisible by $2(q - 1)$, and let α be an element in $GF(q) - \{0\}$ such that the polynomial $x^2 + \alpha x + 1$ is irreducible over $GF(q)$. Then, the difference of any two distinct matrices in the set $\{v_{l,m}\}$ is nonsingular.*

For our particular case:

- Since $q = 2$, $p - 1$ which is an even number is divisible by $2(q - 1) = 2$.
- Since $q = 2$ and $\alpha = 1$, it is trivial to show that $x^2 + x + 1$ is irreducible over $GF(2)$.

From definition 2 and setting parameters $q = 2$ and $\alpha = 1$ (which fulfill Theorem 1), the set of matrices β can be any subset of k matrices in Q_1^i.

Considering a LD-MDS code $C(600, 1200)$ with $k = 2$ and $n = k + 2 = 4$, the parity check matrix for this code can be shown to be as follows:

$$H_\beta = \begin{bmatrix} I & I & I & 0 \\ \beta_1 & \beta_2 & 0 & I \end{bmatrix}, \quad (10)$$

where $\beta = \{\beta_1, \beta_2\}$ is a set of $b \times b$ matrices and $b = 300$. In order to fulfill (P2), we have $b = (p - 1)$ where p is a prime number. As $p = 301$ is not a prime number, we set $p = 151$ leading to $b = 150$ to design a base matrix that is then expanded to the targeted size using a lifting expansion of order 2 (Ryan & Lin, 2009). For the last step, it consists of replacing the '1' elements of the designed parity check base matrix by a permutation matrix of size 2×2, following the classical lifting expansion of protograph based codes. This allows us to achieve a subset of matrices $\beta = \{\beta_1, \beta_2\}$ of size $b' \times b'$ where $b' = 2b = 300$. For this scheme, the CED and CED redundancy data of Figure 1 have to be divided into 4 blocks (as pictured in figure 4). The division into four blocks is required in order to fully benefit from the MDS capability when applying the erasure-decoding algorithm presented in Appendix A in Section A and that is used within the general decoding procedure as given in Figure 6. Indeed, one of the most important advantages of having a sparse parity check matrix by design for the LD-MDS codes is that low-complexity erasure-decoding algorithms are enabled in order to decode the systematic information. The algorithm implemented for this scheme is presented in Appendix A in Section A.
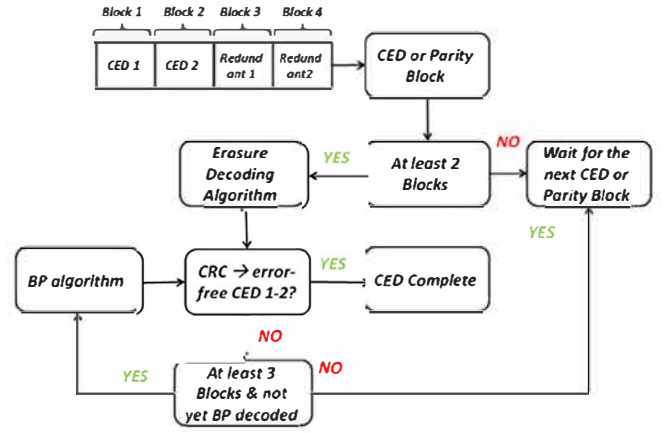

FIGURE 6 LD-MDS and sparse MDS decoding schemes [Color figure can be viewed in the online issue, which is available at wiley-onlinelibrary.com and www.ion.org]

In order to compare the new code with the structure of the GPS L1C or the I/NAV message, we propose to use the structure of GPS L1C. Using this configuration, the CED, which is stored in the subframe 2, is encoded by the proposed LD-MDS code. Moreover, we avoid the use of the interleaver spanning the entire codeword, since it is the main cause of an almost constant TTD in the GPS L1C structure. We now describe the general decoding step, once $k = 2$ blocks of information are received, the erasure algorithm is used to decode the systematic information. In order to check the reliability of the systematic data, a CRC based detection is applied. In case of error, the BP algorithm is performed on the corresponding Tanner graph when more than $k = 2$ information blocks are received. The complete description of the proposed decoding scheme is described in Figure 6.

5.2 | Sparse maximum distance separable (MDS) coding schemes

5.2.1 | Sparse MDS block codes

Lowest-Density MDS codes provide a solution for which the complexity of the decoding algorithm is the lowest possible. However, such codes are not close to the outage boundary under the BP decoding algorithm. The next family of codes aims to enhance the error-correcting capabilities (with respect to the LD-MDS codes) by reducing the sparsity of the parity check matrix.

In order to design a channel-coding scheme that can fulfill the MDS property with some sparsity constraints having coding rate $R = 1/2$ and code structure $C(u, m)$ with $u = 600$ and $m = 1200$, we define the following block

matrix:

$$H_\beta = \begin{bmatrix} H_{1,1} & H_{1,2} & I & 0 \\ H_{2,1} & H_{2,2} & 0 & I \end{bmatrix}, \tag{11}$$

where $H_{1,1}, H_{1,2}, H_{2,1}$ and $H_{2,2}$ are matrices of size $b \times b$ with $b = 300$. As in the case of the LD-MDS codes structure, the CED and the redundant data are divided into four blocks.

Since MDS property allows us to retrieve k data symbols of information from any k error-free symbols, given the matrix structure in Equation (11), we analyze an erasure-block-decoding algorithm that highlights requirements for $H_{1,1}, H_{1,2}, H_{2,1}$ and $H_{2,2}$ for H_β being a sparse MDS code. Note that this algorithm is different from the low-complexity erasure-decoding algorithms tailored for the LD-MDS codes leading to different structures for the codes.

5.2.2 | Modified MDS erasure-block-decoding algorithm

Let us define the received data block from a codeword as Z_i, with $i \in (1, 2, 3, 4)$ being the index related to one of the data blocks which contains a number of symbols equal to b. Then, each of the received data block Z_i can be represented by a binary vector $\underline{Z_i}$ of size $b \times 1$. Following the block structure of the parity check matrix as defined in Equation (11), the two syndrome blocks generated from the received data blocks over $GF(2^b)$ can be computed as:

$$\underline{S_0} = H_{1,1}\underline{Z_1} + H_{1,2}\underline{Z_2} + \underline{Z_3} \tag{12}$$

$$\underline{S_1} = H_{2,1}\underline{Z_1} + H_{2,2}\underline{Z_2} + \underline{Z_4}. \tag{13}$$

Given the fact that a codeword is divided in four data blocks and that the minimum number of received blocks to begin to decode must be at least $k = 2$, the maximum number of erased data blocks is equal to two. Moreover, we define j and t as respectively the lowest and the highest index of the erased data blocks, with $1 \leq j < t \leq 4$. Let us also define the vectors after the decoding of the first and the second block as $\underline{e_1}$ and $\underline{e_2}$ that contain the CED data. Assuming that $H_{1,1}, H_{1,2}, H_{2,1}, H_{2,2}$ are invertible over $GF(2)$, we can now discuss the different configurations that can be encountered:

(a) Case $t = 4$: If $t = 4$, we have the following cases:
- $j = 3$, the information has been already decoded, since the CED is within blocks $\underline{e_1} = \underline{Z_1}$ and $\underline{e_2} = \underline{Z_2}$;
- $j = 2 \rightarrow \underline{S_0} = H_{1,2}\underline{e_2}$, therefore $\underline{e_2} = (H_{1,2})^{-1}\underline{S_0}$ and $\underline{e_1} = \underline{Z_1}$;
- $j = 1 \rightarrow \underline{S_0} = H_{1,1}\underline{e_1}$, therefore $\underline{e_1} = (H_{1,1})^{-1}\underline{S_0}$ and $\underline{e_2} = \underline{Z_2}$.

(b) Case $t = 3$: If $t = 3$, then we have:
- $j = 2 \rightarrow \underline{S_1} = H_{2,2}\underline{e_2}$, therefore $\underline{e_2} = (H_{2,2})^{-1}\underline{S_1}$ and $\underline{e_1} = \underline{Z_1}$;
- $j = 1 \rightarrow \underline{S_1} = H_{2,1}\underline{e_1}$, therefore $\underline{e_1} = (H_{2,1})^{-1}\underline{S_1}$ and $\underline{e_2} = \underline{Z_2}$.

(c) Case $t = 2$: If $t = 2$ and $j = 1$, we finally have:
- Following Equation (12), $\underline{e_1} = (H_{1,1})^{-1}(\underline{S_0} + H_{1,2}\underline{e_2})$;
- Substituting the precedent equation in Equation (13), $\underline{S_1} = H_{2,1}(H_{1,1})^{-1}(\underline{S_0} + H_{1,2}\underline{e_2}) + H_{2,2}\underline{e_2}$;
- Assuming that $(H_{2,1}(H_{1,1})^{-1}H_{1,2} + H_{2,2})^{-1}$ is invertible over $GF(2)$, we obtain $\underline{e_2} = (H_{2,1}(H_{1,1})^{-1}H_{1,2} + H_{2,2})^{-1}(\underline{S_1} + H_{2,1}(H_{1,1})^{-1} + \underline{S_0})$;
- We obtain $\underline{e_1}$ by substituting $\underline{e_2}$ in $\underline{e_1}$.

Therefore, the parity check matrix in Equation (11) must be designed ensuring that $H_{1,1}, H_{1,2}, H_{2,1}, H_{2,2}$ and $(H_{2,1}(H_{1,1})^{-1}H_{1,2} + H_{2,2})$ are invertible over $GF(2)$ to ensure MDS block recovery based on the previous block-erasure-decoding algorithm. To this end, we used a greedy search on the four block matrices $H_{1,1}, H_{1,2}, H_{2,1}, H_{2,2}$. For each of them, we further impose sparsity constraints with a maximum of 4 ones per column while maximizing the girth (minimum cycle length of the corresponding Tanner graph; Ryan & Lin, 2009) for variable nodes belonging to the systematic information part of the parity check matrix.

In order to compare the sparse MDS coding scheme with the structure of the GPS L1C or the I/NAV message, it is proposed to use the structure of GPS L1C. Then, the CED which is stored in the subframe 2 is encoded by the proposed sparse MDS code. Moreover, we avoid the use of the interleaver.

As it was already described for the LD-MDS codes, once $k = 2$ blocks of information are received, the erasure algorithm is used to decode the systematic information (CED). In order to check the reliability of the systematic data, CRC based detection is used. In case of an erroneous solution, the BP decoding is applied when more than $k = 2$ information blocks are received. The decoding scheme is described in Figure 6.

5.3 | Regular root-LDPC codes

We now investigate on the proposed scheme based on regular Root-LDPC codes. These codes belong to a family of codes having both MDS and full diversity properties under the iterative BP decoding algorithm, and they have been initially introduced for the block-fading channel.
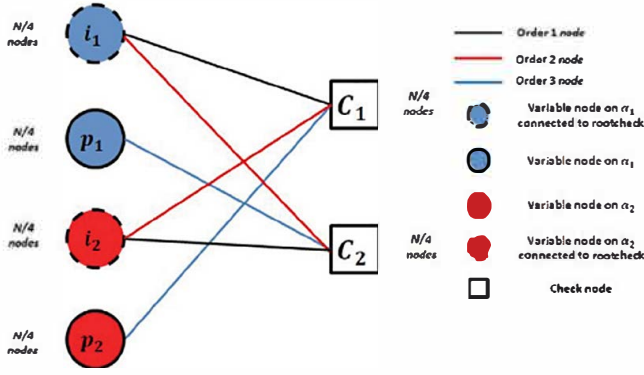
FIGURE 7 Tanner graph for a regular (3,6) root-LDPC code of rate 1/2 [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

The design of the Root-LDPC codes has roots in the limiting case where the fading coefficient can belong to $\mathbb{N} \in \{0, 1\}$, which corresponds to the well-known block-erasure channel. Indeed, it can be shown that usual single parity check nodes involved in LDPC codes do not meet sufficient conditions to tolerate more than one erasure bit as it is shown in Boutros et al. (2010). As a consequence, a new check node structure, referred to as rootcheck node, has been introduced enabling us to tolerate more than one erasure bit under the BP decoding algorithm. In this context, the construction of a regular $(3, 6)$ rootcheck LDPC has been introduced for the case of a block-f $n_c = 2$.

Definition 3 (Boutros et al., 2010). Let x_1 be a binary element transmitted on fading α_1. A rootcheck for x_1 is a checknode $\Phi(x_1, x_2, \dots, x_y)$ where all bits $x_2, \dots, x_y$ are transmitted on fading α_2.

Using Definition 3, the design of a length-N rate-1/2 systematic regular LDPC code that has to operate on a two-blocks fading channel can be summarized as follows. Two classes of bits are first defined, i.e., systematic information bits and redundant parity bits. The $N/2$ systematic information bits are split into two classes: $N/4$ bits (denoted i_1), which are transmitted on the block with fading α_1 and $N/4$ bits (denoted i_2), which are transmitted on the block with fading α_2. Parity bits are also partitioned into two sets (denoted p_1 and p_2, respectively) and sent to the channel following the same assumptions as for the information bits. This mapping of the information and redundant/parity bits is represented in Figure 7 using the bipartite Tanner protograph representation that also shows how the different information and parity bits are connected to rootchecks.

The corresponding block structure of the associated parity check matrix H is directly derived from its Tanner protograph and is given in Equation (14) by

$$H_\beta = \begin{bmatrix} I & 0 & H_{i_2} & H_{p_2} \\ H_{i_1} & H_{p_1} & I & 0 \end{bmatrix}, \qquad (14)$$

where I and 0 are $N/4 \times N/4$ identity and all-zero matrices, respectively. H_{i_k} and H_{p_k}, $k \in (1, 2)$, are sparse regular matrices of Hamming weight 2 and 3 per row and per column, respectively. Examining Equation (14), under the block-erasure channel scenario, we observe that the only outage event occurs when $\alpha_1 = \alpha_2 = 0$ (both blocks erased). Indeed, when $\alpha_1 = 0$ and $\alpha_2 = 1$, it is straightforward to see that information bits i_1 are determined using rootchecks c_1. Similarly, when $\alpha_1 = 1$ and $\alpha_2 = 0$, information bits i_2 are determined using rootchecks c_2.

Finally, two methods to generate the parity matrices have been used:

- The first method is based on the design of parity check matrices using a modified Progressive Edge Growth (PEG) algorithm that enables us to take into account local constraints following (Uchôa, Healy, Lamare, & Souza, 2011).
- The second method considers the design of Quasi-Cyclic (QC) matrices following, for example, Li and Salehi (2010).

From Definition 3, it is trivial that the data structure of a regular Root LDPC (3,6) code must be divided into two different blocks, each one corresponding to α_1 or α_2. Once one of the blocks is received, the decoding process starts by executing the BP algorithm. In case of decoding a correct CRC, the CED is retrieved, otherwise another block must be received. The decoding scheme is described in Figure 8.

5.4 | Irregular protograph root-LDPC codes scheme

In this section, we investigate on the design of irregular Root LDPC codes based on protographs (Thorpe, 2003). A protograph is a Tanner graph G for which parallel edges are permitted. In order to generate a LDPC code from a protograph, a *copy and permute* operation also called lifting is used to interleave multiple copys of the original protograph (Thorpe, 2003). LDPC codes generated from protographs can enhance the error-correcting performance compared to Regular LDPC codes, since good irregular LDPC codes can be designed.
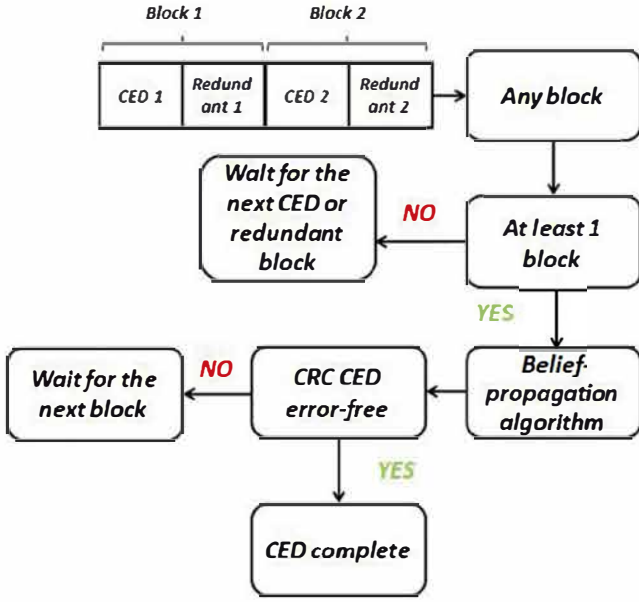
FIGURE 8 Root-LDPC decoding scheme [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

Let us now introduce the so-called base matrix H_B associated with the protograph of the regular Root LDPC code given by Equation (14). The base matrix H_B is given by

$$H_B = \begin{bmatrix} 1 & 0 & 2 & 3 \\ 2 & 3 & 1 & 0 \end{bmatrix}. \tag{15}$$

In this representation, the coefficient $H_B(j, i)$ represents the number of connections/edges between the i-th column and the j-th row of the base matrix. Each column i is associated to a group of variable nodes while each row j is associated to a group of check nodes in the final parity-check matrix. All nodes belonging to the same group, also referred to as class or type, share the same local connection properties. Based on the type of local connections you can have (represented by the coefficients $H_B(j, i)$), variable nodes (respectively check nodes) can be divided into different classes/types. For the regular Root LDPC code, all variable nodes are of degree 3 (they are all connected to exactly 3 check nodes), while check nodes are all of degree 6 (they are all connected to exactly 6 variable nodes). But, when considering the detailed connections between possible groups of variable nodes and check nodes, we can define 4 different types/classes of variable nodes denoted (i_1, p_1, i_2, p_2) and two types/classes of check nodes denoted (c_1, c_2). For example, using this protograph representation, variable nodes of type i_1 are exactly connected to one check node of type/class c_1 and two of class c_2. Variable nodes of type p_1 are only connected to three check nodes of type/class c_2. This is a classical representa-

tion for protograph-based codes. Analyzing the threshold of the regular Root-LDPC code using the Protograph EXIT (PEXIT) Chart algorithm (Liva & Chiani, 2007), a demodulation threshold loss of 0.4 dB with respect to the GPS L1C demodulation threshold is obtained. In order to enhance the demodulation threshold, we now present the design of irregular Root-LDPC codes to protect the CED of the navigation message.

To do so, we adopt the following general protograph representation for a Root-LDPC code of rate $R = 1/2$:

$$H_B = \begin{bmatrix} 1 & 0 & * & * \\ * & * & 0 & 1 \end{bmatrix}, \tag{16}$$

where $*$ represents connection weights $\in \mathbb{N}$ to be optimized. In order to enhance the error-correction performance of the regular Root-LDPC code, we can use the Protograph EXIT (PEXIT) Chart algorithm (Liva & Chiani, 2007) to search for coefficients $*$ in Equation (16), which reduce the demodulation threshold. We can also note that in order to limit the search space, only matrix weights in the subset $\in (0, 1, 2, 3)$ are considered as done, for example, in Fang, Bi, and Guan (2014). In Fang et al. (2014), some optimized protograph structures have been presented; however, small gains in the demodulation threshold with respect to the regular Root-LDPC codes have been observed. To enhance the demodulation threshold gains, Fang et al. (2014) rather considered the following lifted protograph representation:

$$H_{\beta_1} = \begin{bmatrix} 1 & 0 & 0 & 0 & * & * & * & * \\ 0 & 1 & 0 & 0 & * & * & * & * \\ * & * & * & * & 1 & 0 & 0 & 0 \\ * & * & * & * & 0 & 1 & 0 & 0 \end{bmatrix}, \tag{17}$$

where $*$ represents coefficient weights $\in (0, 1, 2, 3)$ to be optimized.

The optimized protograph structure in Fang et al. (2014) has been designed to have good error-correcting capabilities in the block-fading channel. However, this protograph structure does not provide the minimum demodulation threshold in the ergodic channel. Since a low demodulation threshold is crucial for the retrieval of the CED, in Equation (18), we rather search for a protograph structure which minimizes the demodulation threshold given the required Root protograph structure given in Equation (17). The obtained base matrix is as follows:

$$H_B = \begin{bmatrix} 1 & 0 & 0 & 0 & 2 & 1 & 3 & 0 \\ 0 & 1 & 0 & 0 & 2 & 0 & 3 & 1 \\ 1 & 3 & 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 3 & 2 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}. \tag{18}$$

We can note that the proposed protograph structures in Fang et al. (2014) and in Equation (18) are both asymmetric. Therefore, the error-correcting capabilities lead to unequal block recovery for the different variable node types. Since an unequal recovery may affect directly the TTD performance, especially in a good channel environment, we have optimized the protograph enforcing a symmetric structure, which minimizes the demodulation threshold given the required Root protograph structure given in Equation (17). The resulting base matrix is given by

$$H_{\beta_1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 3 & 1 & 2 \\ 0 & 1 & 0 & 0 & 0 & 3 & 1 & 1 \\ 1 & 3 & 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 3 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}. \tag{19}$$

Finally, LDPC codes matrices expanded from the proposed root-protograph codes are obtained using classical lifting based expansion methods (Ryan & Lin, 2009).

6 | EVALUATION FOR THE BLOCK RAYLEIGH FADING CHANNEL

In this section, in order to illustrate the notion of diversity, we present the performance of the proposed channel-coding schemes over the block Rayleigh fading channel, i.e., the independent fading channel coefficients follow a normalized Rayleigh fading distribution.

In Figure 9, we have illustrated the CED error rate (CEDER) for the irregular LDPC code of GPS L1C subframe 2 (red/solid line), the LD-MDS code with $R = 1/2$, the sparse MDS code with $R = 1/2$ (yellow/dash-circle line), the sparse MDS codes with rate $R = 1/2$ (cyan/dash-pentagon line); the Irregular LDPC code of GPS L1C subframe 2 with the GPS L1C block interleaver (orange/dash-point-cross line); the regular (3,6) Root code with rate $R = 1/2$ (green/dash-plus line); the irregular Protograph Root code with rate $R = 1/2$ (blue/dash-cross line), and the irregular symmetrical Protograph Root code with rate $R = 1/2$ (magenta/dash-diamond line). For this simulation, we are considering a block-fading channel with $n_c = 2$, for which each block-fading coefficient follows a normalized Rayleigh distribution. Then, the Outage Probability P_{out} for a BPSK input with $R = 1/2$ and block-fading channel $n_c = 2$ (black/solid line) is also illustrated.

On the one hand, we notice that all the coding schemes with Root structure provide the same slope as the outage probability curve (achieving full diversity), and the distance from the outage bound characterizes the strength of the different schemes. It also underlines that they do not achieve the optimal coding gain. On the other hand,
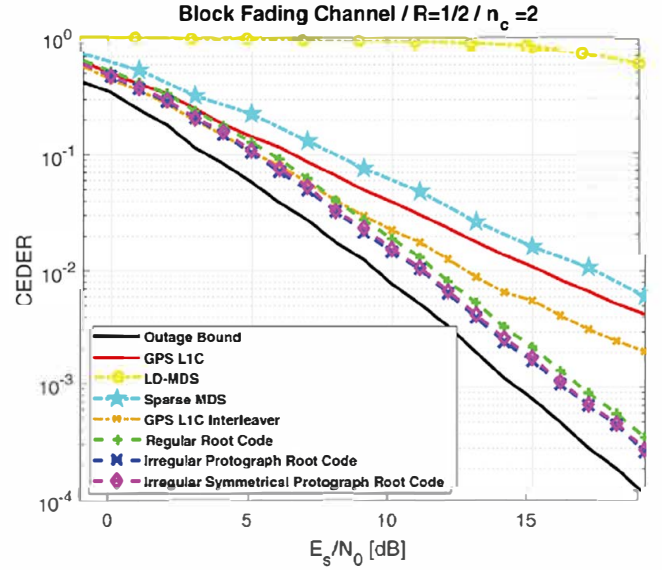

FIGURE 9 CEDER of the proposed channel-coding schemes for a BPSK input over a block Rayleigh fading channel with $n_c = 2$ [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

the error probability curves corresponding to the LD-MDS and sparse MDS cases show that those coding schemes do not achieve full diversity over the block Rayleigh fading channel (lower slope than the outage probability curve). We also see an improvement of the error-correcting performance provided by the sparse MDS code structure with respect to the LD-MDS structure. Furthermore, the curves from the irregular LDPC code of GPS L1C subframe 2 and the irregular LDPC code of GPS L1C subframe 2 with the block interleaver of GPS L1C provide a lower slope than the Root structures since no full diversity is achieved. Note that the block interleaver generates a channel average effect, enhancing the diversity of the channel-coding scheme. In any case, the block interleaver does not provide full diversity, when a block-fading channel with $n_c = 2$ is considered. Moreover, it must be pointed out that the block interleaver enforces the reception of the *entire* codeword in order to decode the CED, delaying the CED decoding and consequently increasing the TTD. On the contrary, the Root code structure (see Figure 8) needs only one block to decode the CED, minimizing the TTD.

Since the block interleaver enforces a structure not able to reduce the TTD, we now study the GPS L1C subframe 2 without interleaver (considering only the irregular LDPC code). In this context, we compare the error-correcting performance between the irregular LDPC code of GPS L1 subframe 2 (CED allocated in the first block and the redundant data allocated in the second block) and the Root code structures (half of the CED and the redundant data are allocated in the first block and the other half of the CED and the
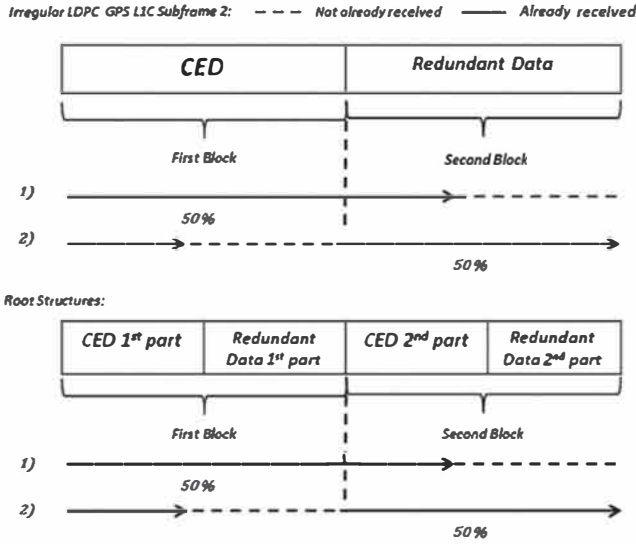
FIGURE 10 Model at the receiver for the Irregular LDPC code of GPS L1C subframe 2 and the Root codes structure as a function of the received percentage of the codeword
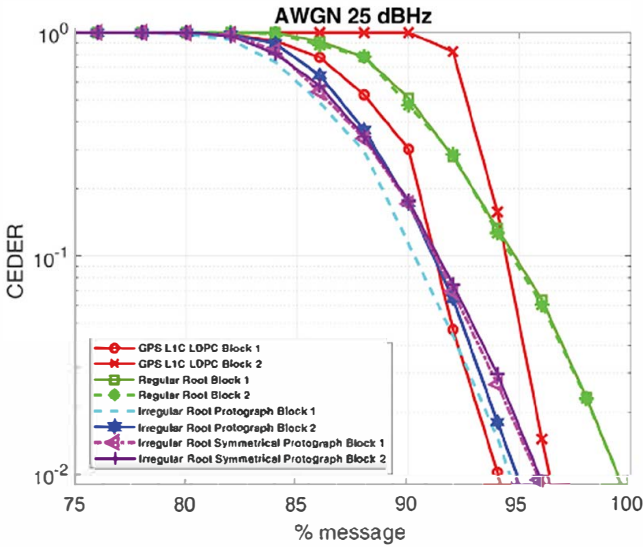

FIGURE 11 CEDER vs message percentage over an AWGN channel with $C/N_0 = 25$ dBHz of some of the proposed channel-coding scheme when the first or the second block is totally received [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

redundant data are allocated in the second block) considering the reception models as described in Figure 10. Those models consider an AWGN channel where a percentage of the codeword is not yet received (labelled as erasured). Then, in Figure 11 and Figure 12, the CEDER is illustrated as a function of the received percentage (%) of the codeword over an AWGN channel with a $C/N_0 = 25$ dBHz (Figure 11) and a $C/N_0 = 30$ dBHz (Figure 12), considering that the first or the second block has already been
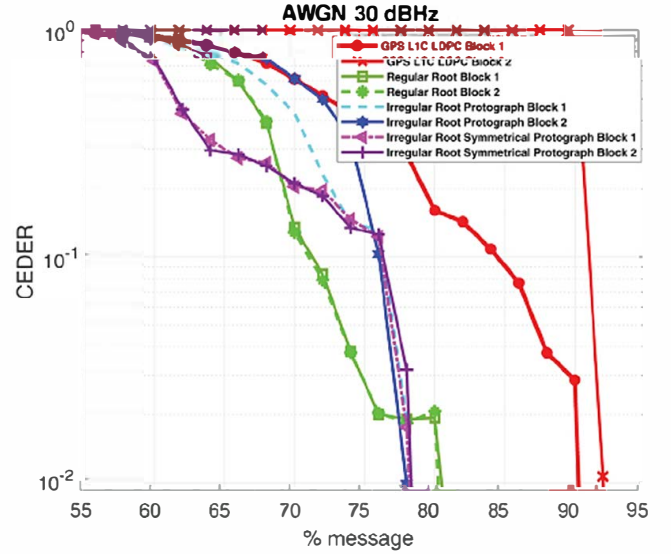

FIGURE 12 CEDER vs message percentage over an AWGN channel with $C/N_0 = 30$ dBHz of some of the proposed channel-coding scheme when the first or the second block is totally received [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

received. We can notice that the Root code schemes provide a lower demodulation threshold with a smaller percentage of the received codeword than the irregular LDPC code of GPS L1C subframe 2. As a remarkable example (Figure 12, $C/N_0 = 30$ dBHz), the irregular LDPC code of GPS L1 subframe 2 needs more than 90% of the codeword to converge to the CEDER of 10^{-2}. On the other hand, the regular Root code structure converges to a CEDER of 10^{-2} with only 81% of the codeword. This percentage decreases to 76% of the codeword when irregular Root structures are used. These experiments show how the Root structure enables us to improve the TTD.

6.1 | Effect of the interleaver

Considering the irregular LDPC code of GPS L1C subframe 2 with the block-interleaver structure of GPS L1C over the block-fading channel with $n_c = 2$, the block interleaver does not provide full diversity. However, the block interleaver helps to average the channel, increasing the diversity compared to the case where no interleaving is considered at all. Concerning the proposed Root structure, full diversity is only achieved when the number of fading blocks is equal to $n_c = 2$. Otherwise, considering a block-fading channel with $n_c > 2$, the proposed Root structure does not provide full diversity with the BP algorithm. In Figures 13 and 14, CED error rates are illustrated for different code families (the irregular GPS L1C subframe 2 LDPC code, the irregular GPS L1C subframe 2 LDPC with
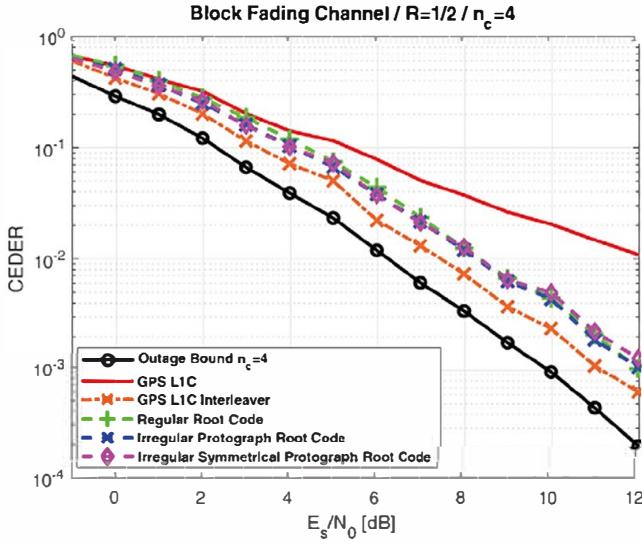
FIGURE 13 CEDER of the proposed channel-coding schemes for a BPSK input over a block Rayleigh fading channel with $n_c = 4$ [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]
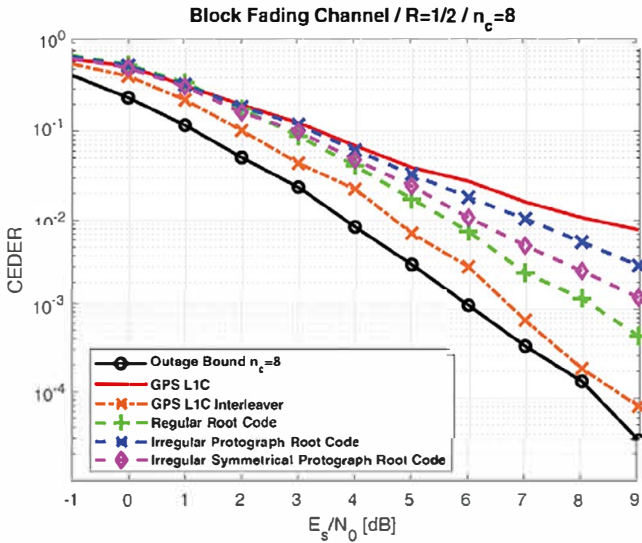

FIGURE 14 CEDER of the proposed channel-coding schemes for a BPSK input over a block Rayleigh fading channel with $n_c = 8$ [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

the GPS L1C block interleaver, the regular (3,6) Root code with $R = 1/2$, the irregular Protograph Root code with $R = 1/2$, and the irregular symmetrical Protograph Root code with $R = 1/2$) considering $n_c = 4$ and $n_c = 8$. Each of the fading gains follows a normalized Rayleigh distribution. From these Figures, we see that the block interleaver enhances the diversity (due to the fact that the block interleaver enables us to average the information over the fading blocks) and, consequently, the error-correction
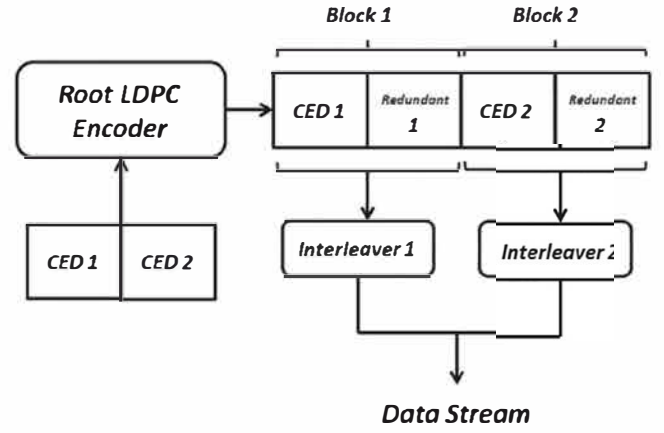

FIGURE 15 Encoding Structure of the Root LDPC codes with rate $R = 1/2$ considering two independent block interleavers for each of the transmitted data blocks

performance for the interleaved version of GPS L1C. Moreover, as expected, we see that the Root code structures with $R = 1/2$ does not provide full diversity when $n_c > 2$ for the BP algorithm, yielding decreased error-rate performance (please refer to Figures 13 and 14).

However, we can do better for the root structure in the case where $n_c > 2$ by considering, as for the GPS L1C, a strategy of a structured channel interleaving to overcome the loss of full diversity. Having a block interleaver along the entire codeword will result in roughly the same results as those for for GPS L1C. But it will also enforce us to receive the entire codeword to decode the CED, and we will lose the benefit from the Root structure for fast recovering. To overcome this issue, we propose to add two independent block interleavers to each of the output blocks provided by the Root code structure (the scheme is illustrated in Figure 15). Adding those sub-block interleavers helps to enhance the average diversity at the receiver on each part of the Root codeword, improving the error-correcting performance and closing the gap with the performance of GPS L1C. Moreover, since each interleaver is applied independently to each of the output blocks (half part of the Root codewords), the decoding scheme presented in Figure 8 can be integrated at the receiver, allowing a decoder structure that can reduce the TTD. To illustrate this point, Figures 16 and 17 give the CEDER for the irregular GPS L1C subframe 2 LDPC code, the irregular GPS L1C subframe 2 LDPC with the GPS L1C block interleaver, the regular (3,6) Root code with $R = 1/2$ and with two independent block interleavers, the irregular Protograph Root code with $R = 1/2$ and with two independent block interleavers and the irregular symmetrical Protograph Root code with $R = 1/2$ and with two independent block interleavers, considering $n_c = 4$, and $n_c = 8$. Each of the fading gains follows a normalized Rayleigh distribution. From these
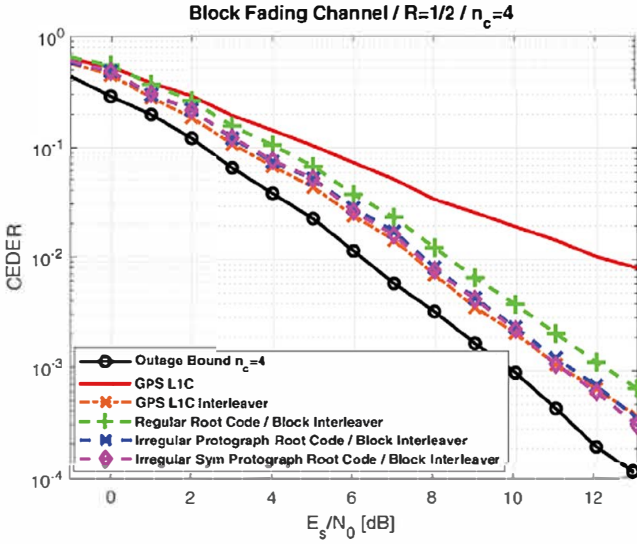
FIGURE 16 CEDER of the proposed channel-coding schemes (with block interleaver) for a BPSK input over a block Rayleigh fading channel with $n_c = 4$ [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]
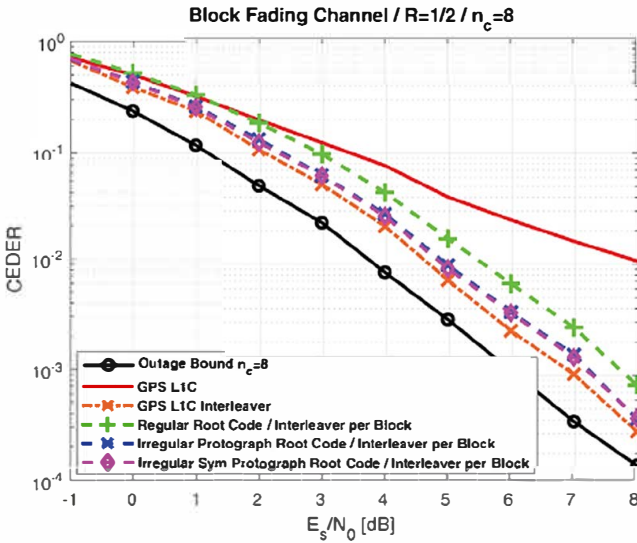

FIGURE 17 CEDER of the proposed channel-coding schemes (with block interleaver) for a BPSK input over a block Rayleigh fading channel with $n_c = 8$ [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

figures, we can notice an enhancement of the decoder diversity thanks to the structured block interleaver, providing almost the same error-correcting performance than the irregular GPS L1C subframe 2 LDPC with the GPS L1C block interleaver. The irregular GPS L1C subframe 2 LDPC with the GPS L1C block interleaver provides slightly better performance due to: (a) its block interleaver averages the block channel over the entire codeword, and (b) the irregularity of the underlying LDPC code gives better thresholds due to a higher maximum variable node

degree. By considering higher variable node degrees for the design, performance of our irregular schemes could be improved. As expected, the regular Root structure provides worse error-correcting performance than the irregular structures due to its higher demodulation threshold. Finally, we can remark that even if the proposed Root structures provide slightly worse error-correcting performance over the block-fading channel with $n_c > 2$, thanks to this structure, the decoder is able to reduce the TTD, which is the final objective of this work.

7 | EVALUATION FOR STANDARD SCENARIOS

In order to compare the performance of the error-correcting solutions proposed in Section 5, CEDER and the TTD are evaluated over the AWGN channel and the urban channel.

7.1 | Retrieved CED error rate

We first consider an AWGN channel. This model does not include fading or interferences coming from other sources. At the receiver, after sampling, the received baseband signal can be written as:

$$y_k = x_k + n_k \qquad (20)$$

where y_k is the received signal, x_k is the transmitted signal, and n_k is the centered AWGN noise with noise variance σ^2, i.e., $n_k \sim \mathcal{N}(0, \sigma^2)$.

For our performance evaluation, we assume that the entire codeword has been received. Figure 18 illustrates the CEDER in terms of C/N_0 for GPS L1C, the Galileo E1B I/NAV message, the proposed RS2 configuration of the I/NAV message, the LD-MDS codes, the sparse MDS codes, the regular Root-LDPC QC code structure, the regular Root-LDPC PEG code structure, the irregular Root Protograph code structure, and the irregular Root Protograph code with a symmetric structure.

Simulation results show that regular Root-LDPC codes obtain the best demodulation threshold compared to the Galileo E1B I/NAV message, the RS2 configuration of Galileo E1B I/NAV message, the LD-MDS codes, and sparse MDS codes with a demodulation threshold gain of 2.5 dBHz, 0.4 dBHz, 6 dBHz, and 0.9 dBHz, respectively, for a targeted error probability of 10^{-2}. Moreover, an irregular Protograph Root-LDPC code and an irregular Protograph Root-LDPC code with a symmetric structure, designed using the PEXIT charts (Liva & Chiani, 2007; Ryan & Lin, 2009), are simulated. Such irregular codes
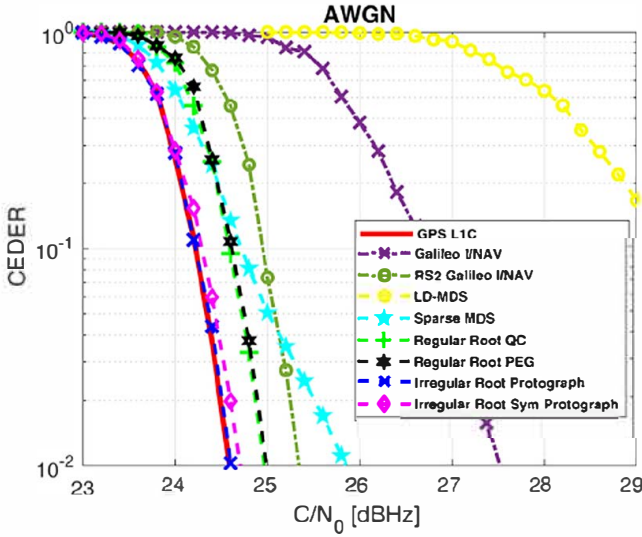
FIGURE 18 CEDER over an AWGN channel [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

FIGURE 19 CEDER over the LMS channel modeled using the two-state Prieto model for a vehicle speed of 40 km/h and an elevation angle of 40 degrees [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

reduce the demodulation threshold compared to the regular Root LDPC by 0.4 dBHz and achieve the same decoding performance as GPS L1C. It must be noted that thanks to the Root LDPC structure (regular or irregular), a reduction of the TTD without degrading the demodulation threshold can be achieved (or with a negligible degradation in the case of regular Root LDPC). Note that simulation results in Figure 18 are presented without block-interleaver structures since no gain is achieved over the AWGN channel.

Secondly, we present CEDER considering an urban environment modeled using the two-state Prieto model (Prieto-Cerdeira et al., 2010) for a vehicle speed of 40 km/h and an elevation angle of 40 degrees. In Figure 19, CED error rate is reported for the LMS channel as a function of the C/N_0 considering the following schemes: the Irregular LDPC code of GPS L1C subframe 2 with and without the GPS L1C block interleaver, the sparse MDS codes, the irregular symmetrical Protograph Root code, and the irregular symmetrical Protograph Root code with two independent block interleavers (please refer to the structure presented in Figure 15). We can see that the irregular LDPC code of GPS L1C subframe 2 using the GPS L1C block interleaver, the Irregular Root Protograph code, and the Irregular Symmetrical Root Protograph code has similar performance. Moreover, the sparse MDS code presents a gap of 1 dB with respect to the irregular LDPC code of GPS L1C subframe 2 with the GPS L1C block interleaver. From Figure 19, it can be seen that the block interleaver in the GPS L1C structure and the two block interleavers in the irregular symmetrical Protograph Root structure only provide a slight enhancement of the error-correcting performance (0.05 dBHz and 0.2 dBHz, respectively). It shows that due to the fact that
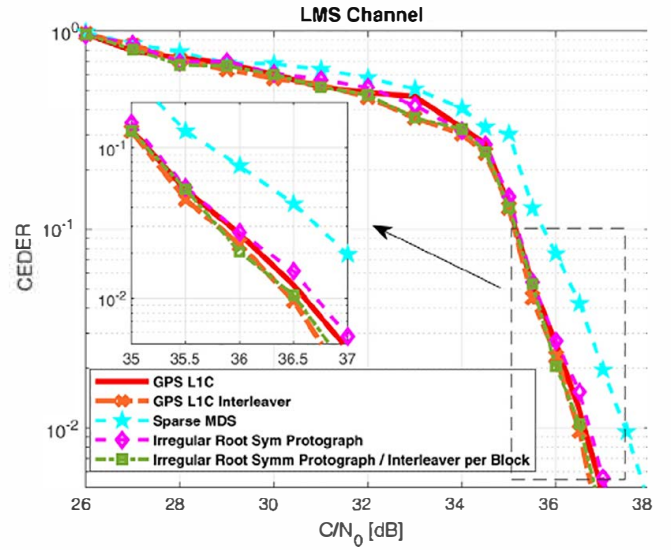
the LMS channel is a very "volatile" channel, an interleaver seems to have a negligible effect on the decoding performance.

7.2 | Time to data (TTD)

The TTD gives an indication of the time required by the receiver to correctly retrieve the CED from the navigation message, starting from the first epoch at which the first data symbol is extracted from the receiver. The following analysis considers the following assumptions:

- TOW is assumed to be known.
- The results are expressed in terms of the TTD values.

In order to obtain the TTD values, we need to define the Probability Density Function (PDF) $f(t)$ of the TTD. The TTD can then be obtained from the Cumulative Distribution Function (CDF) defined as follows:

$$CDF(TTD) = \int_{-\infty}^{TTD} f(t)dt = x, \qquad (21)$$

where x describes the percentage of confidence needed in order to represent the time needed by the receiver to retrieve CED. For simulations, we first evaluate 100.000 times the duration needed by one receiver to obtain the error-free CED for each of the proposed error-correcting solutions considering an AWGN channel with $C/N_0 = 25$ dBHz, $C/N_0 = 30$ dBHz, and $C/N_0 = 45$ dBHz. As expected, the first epoch (first synchronized bit) can arrive
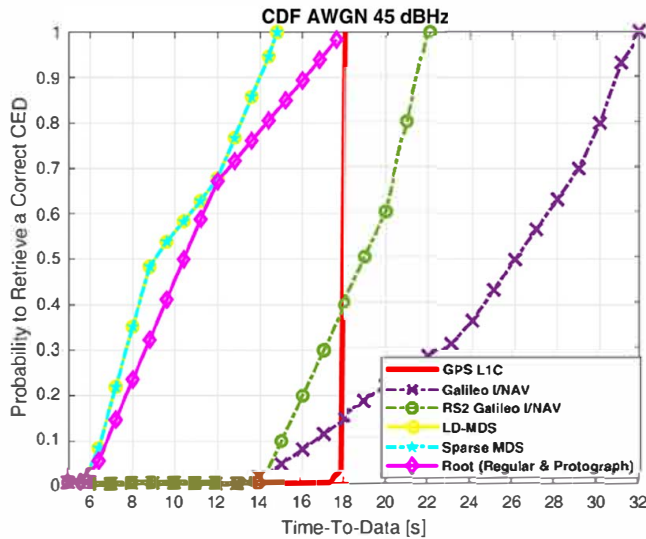
FIGURE 20 TTDs over AWGN channel with a $C/N_0 = $ 45 dBHz [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

FIGURE 21 TTDs over AWGN channel with a $C/N_0 = $ 30 dBHz [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

at any time. In order to initialize the first epoch value for each of the 100.000 simulations, the start symbol is sampled uniformly in the interval defined by the first and the last symbol of the nominal subframe structures.

The error-correcting schemes along with the new message structure are simulated and compared to each other as well as to the Galileo E1B I/NAV, RS2 configuration of Galileo E1B I/NAV and GPS L1C message structure under the AWGN channel assumption. In order to evaluate the reduction of the TTD, an analysis of the time to retrieve the CED based on the calculation of the cumulative distribution function (CDF) is implemented. Simulation results are presented in Figure 20, Figure 21, and Figure 22, respectively.

Simulation results in Figure 20 show that the Galileo E1B I/NAV and the RS2 configuration of Galileo E1B I/NAV have higher TTDs than the GPS L1C message structure. Moreover, it is shown as a reduction of more than 30% of for at least 66% of the time compared to the current GPS L1C signal and a reduction of 50% of TTD for at least 30% of the time in case of Root-LDPC scheme (under high $C/N_0 = $ 45 dBHz channel conditions). Those results are even better in the case of LD-MDS and sparse MDS schemes, where simulations show a reduction of 50% of TTD for at least 50% of the time compared to the current GPS L1C signal. The main reason for the improvement of the TTD performance is due to the MDS property. Thanks to this property, under good channel conditions, the proposed error-correcting schemes are able to reduce the time to retrieve the CED since not all the data (redundant or systematic) need to be recovered to decode. Moreover, the sparse MDS and LD-MDS schemes provide better results in terms of
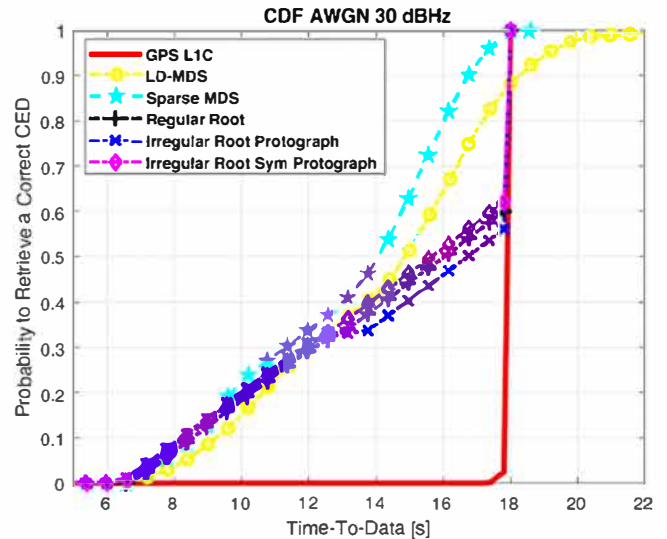

FIGURE 22 TTDs over AWGN channel with a $C/N_0 = $ 25 dBHz [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]
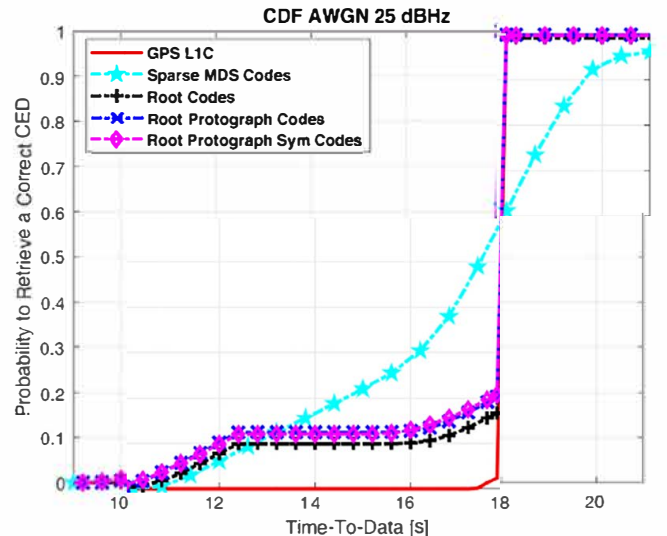
TTD compared to the Root codes as the MDS property works for any of the four blocks of the message structure. Since the message structure of the Root codes requires a separation of the redundant and systematic information in a maximum of two blocks in the considered cases, there is not as many degrees of freedom as for the sparse MDS or LD-MDS codes. In Table 1, we illustrate the TTD relevant parameters for a better comparison between proposed message structures.

Since the Galileo E1B I/NAV and the RS2 configuration of Galileo E1B I/NAV have higher TTDs than the GPS L1C message structure, in the following, we compare the

TABLE 1 TTDs revelant results considering $C/N_0 = 45$ dBHz, $C/N_0 = 30$ dBHz, and $C/N_0 = 25$ dBHz

C/N_0	45 dBHz	45 dBHz	30 dBHz	30 dBHz	25 dBHz	25 dBHz
Message Structure	Average TTD	TTD 95%	Average TTD	TTD 95%	Average TTD	TTD 95%
GPS L1C	18 s	18 s	18 s	18 s	18 s	18 s
Galileo E1B I/NAV	26.5 s	31.6 s	–	–	–	–
RS2 Galileo E1B I/NAV	19 s	21.75 s	–	–	–	–
LD- MDS	9 s	14.6 s	14.9 s	19.1 s	–	–
Sparse MDS	9 s	14.6 s	14.1 s	17.1 s	17.5 s	20.4 s
Regular Root	10.4 s	17 s	16.1 s	18 s	17.9 s	18 s
Irregular Root Protograph	10.4 s	17 s	16.8 s	18 s	17.9 s	18 s
Irregular Root Sym Protograph	10.4 s	17 s	15.6 s	18 s	17.9 s	18 s

proposed scheme only with respect to the GPS L1C message structure. In Figure 21, it is shown that the CDF of the different proposed schemes for a $C/N_0 = 30$ dBHz. A decrease of the TTD for at least 60% of the time compared to the current GPS L1C signal is shown for the case of Root codes and a decrease of TTD for at least 90% of the time in the case of the LD-MDS scheme. Under this channel condition, it is shown that the sparse MDS candidate provides a better solution in all cases. It must also be noted that the LD-MDS solution performs worse than the sparse MDS one as the error-correcting capabilities of the sparse MDS code are higher than the error-correcting capabilities of the LD-MDS. Note also that the Protograph Root LDPC code with a symmetric structure (regular or irregular) outperforms the Protograph Root code with an asymmetric structure since those codes provide unequal protection for each data block. Therefore, those codes increase the average TTD when the less protected block is first received. In Table 1, we illustrate the TTD relevant parameters for a better comparison between proposed message structures.

In Figure 22, it is shown that the CDF of the error-correcting candidate for a $C/N_0 = 25$ dBHz, which can be considered as low AWGN carrier-to-noise ratio conditions. A small reduction of the TTD, for almost 20% of the cases, is shown for Root codes, compared to the current GPS L1C signal. Otherwise, the same performance as the GPS L1C channel-coding scheme is reached. The reason for which the Root codes are capable of reaching the same performance as the GPS L1C channel-coding scheme is due to the full diversity property, which provides to the Root codes notable error-correcting capabilities under low carrier-to-noise ratio conditions. It should be noticed that irregular Root-LDPC protograph codes achieve the best performance in terms of TTD compared to the other Root-LDPC codes, since the threshold and the error-correcting capabilities of the codes are better. For the sparse MDS code scheme, a reduction of the TTD is reached, for at least 60% of the cases, thanks to the MDS property. However, since under BP algorithm the sparse MDS code scheme does not have the full diversity property, a reduction in

the error-correcting capabilities are observed and a higher TTD is shown in the remaining cases. It should be noticed that the LD-MDS solution is not presented in Figure 22; this is because the LD-MDS codes do not converge for low AWGN carrier-to-noise ratio conditions due to poor error-correcting capabilities. In Table 1, we illustrate the TTD relevant parameters for a better comparison between proposed message structures.

In a second experiment, we evaluate 100.000 times the duration needed by one receiver to obtain the error-free CED for each of the proposed error-correcting solutions considering an urban scenario modeled through the two-state Prieto model for a vehicle speed of 40 km/h and an elevation angle of 40 degrees with $C/N_0 = 40$ dBHz and $C/N_0 = 37$ dBHz. As expected, the first epoch (first synchronized bit) can arrive at any time. Then, as it was proposed for the AWGN channel, we initialize the first epoch value considering that the start symbol is sampled uniformly in the interval defined by the first and the last symbol of the nominal subframe structures.

In Figure 23, we have studied the TTD for an urban environment modeled through the two-state Prieto model (Prieto-Cerdeira et al., 2010) for a vehicle speed of 40 km/h and an elevation angle of 40 degrees with a $C/N_0 = 37$ dBHz. We remark that the Root codes structures reduce the TTD with respect to the GPS L1C subframe 2. Sparse MDS codes provide better results than other code structures until the 75% of the case. Then, they are performing worse than others. In Table 2, we have illustrated the TTD relevant parameters for a better comparison between proposed message structures.

Finally, in Figure 24, we give the TTD over an urban environment modeled through the two-state Prieto model (Prieto-Cerdeira et al., 2010) for a vehicle speed of 40 km/h and an elevation angle of 40 degrees with a $C/N_0 = 40$ dBHz. We remark that the Root code structures reduce the TTD with respect to the GPS L1C subframe 2. Sparse MDS codes provide better results than other code structures until the 94% of the case. Then, they are performing worse than others. In Table 2, we have illustrated the TTD

TABLE 2 TTDs revelant results considering $C/N_0 = 37$ dBHz and $C/N_0 = 40$ dBHz

C/N_0	37 dBHz	37 dBHz	37 dBHz	40 dBHz	40 dBHz	40 dBHz
Message Structure	TTD 25%	Average TTD	TTD 95%	TTD 25%	Average TTD	TTD 95%
GPS L1C	18 s	18 s	18 s	18 s	18 s	18 s
Sparse MDS	12.5 s	17.8 s	21.6 s	10.4 s	14.1 s	18.2 s
Regular Root QC	14.6 s	17.9 s	18 s	11.2 s	17 s	18 s
Irregular Root Sym Protograph	14.2 s	17.9 s	18 s	11.2 s	17 s	18 s
Irregular Root Sym Protograph/Interleaver per Block	14.2 s	17.9 s	18 s	11.2 s	17 s	18 s

FIGURE 23 TTD over the LMS channel modeled using the two-state Prieto model for a vehicle speed of 40 km/h and an elevation angle of 40 degrees with a $C/N_0 = 37$ dBHz [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]
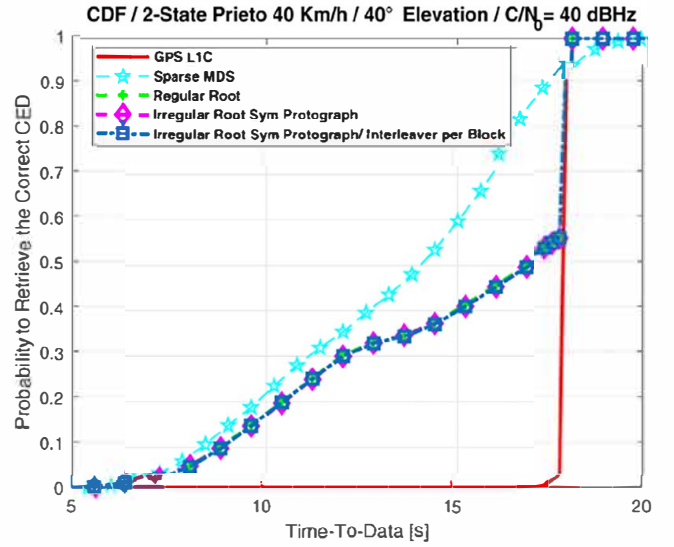

FIGURE 24 TTD over the LMS channel modeled using the two-state Prieto model for a vehicle speed of 40 km/h and an elevation angle of 40 degrees with a $C/N_0 = 40$ dBHz [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

relevant parameters for a better comparison between proposed message structures.

8 | CONCLUSION

In this paper, four different error-correcting schemes have been proposed that enable us to jointly benefit from the navigation message structure and some advanced channel-coding properties. This design approach, referred to as co-design, enables us to reduce the TTD and to provide enhanced error-correction capabilities under low C/N_0 environments. In order to design such schemes, MDS and full diversity properties are required under the non-ergodic (erasure) channel assumption. Simulation results show that co-designing the message structure with LD-MDS and sparse MDS codes provides an efficient solution in order to reduce the TTD under good channel conditions thanks to the MDS property and the erasure-decoding algorithm, but

increases the TTD under harsh channel conditions, since those codes are not of full diversity under the BP decoding algorithm. On the other hand, co-designing the message structure with Root code structures with $R = 1/2$ provides a good solution in order to reduce the TTD without degrading the error-correction performance under low C/N_0 environments. Indeed, those codes are shown to be MDS and full diversity over the block-fading channel with $n_c = 2$, when the BP decoding algorithm is applied. Moreover, in order to improve the demodulation threshold of regular Root-LDPC codes, irregular Root-LDPC codes have been investigated and designed. In order to provide a robust structure over a more general block-fading channel $n_c > 2$, it has been proposed to add two independent block interleavers to each of the output blocks provided by the Root code structure. That helps to enhance the decoder diversity and consequently the error-correction performance over the block-fading channel. Finally, we provide results over standard scenarios such as AWGN

channel and LMS channel, displaying the benefits to use the proposed co-design schemes in order to both: reduce the TTD and improve the resilience of the CED.

ORCID
Lorenzo Ortega https://orcid.org/0000-0002-7650-5967
Charly Poulliat https://orcid.org/0000-0001-6407-8841
Marie Laure Boucheret https://orcid.org/0000-0001-6033-1766

REFERENCES
Biglieri, E., Proakis, J., & Shamai, S. (1998). Fading channels: Information-theoretic and communications aspects. *IEEE Transactions on Information Theory*, 44(6), 2619–2692. https://doi.org/10.1109/18.720551

Blaum, M., & Roth, R. M. (1999). On lowest density MDS codes. *IEEE Transactions on Information Theory*, 45(1), 46–59. https://doi.org/10.1109/18.746771

Boutros, J. J., Fàbregas, A. G., Biglieri, E., & Zémor, G. (2010). Low-density parity-check codes for nonergodic block-fading channels. *IEEE Transactions on Information Theory*, 56(9), 4286–4300. https://doi.org/10.1109/TIT.2010.2053890

Fabregas, A. G., & Caire, G. (2006). Coded modulation in the block-fading channel: Coding theorems and code construction. *IEEE Transactions on Information Theory*, 52(1), 91–114. https://doi.org/10.1109/TIT.2005.860414

Fang, Y., Bi, G., & Guan, Y. L. (2014). Design and analysis of root-protograph LDPC codes for non-ergodic block-fading channels. *IEEE Transactions on Wireless Communications*, 14(2), 738–749. https://doi.org/10.1109/TWC.2014.2359221

IS-GPS-800. (2018). *Interface specification IS-GPS-800 NavStar GPS space segment/usersegment L1C interface*. Retrieved from https://www.gps.gov/technical/icwg/IS-GPS-800E.pdf

Knopp, R., & Humblet, P. A. (2000). On coding for block fading channels. *IEEE Transactions on Information Theory*, 46(1), 189–205. https://doi.org/10.1109/18.817517

Li, Y., & Salehi, M. (2010). Quasi-cyclic LDPC code design for block-fading channels. In *44th Annual Conference on Information Sciences and Systems (CISS)*, pp. 1–5. https://doi.org/10.1109/CISS.2010.5464729

Liva, G., & Chiani, M. (2007). Protograph LDPC codes design based on EXIT analysis. In *IEEE GLOBECOM 2007 - IEEE Global Telecommunications Conference*, pp. 3250–3254. https://doi.org/10.1109/GLOCOM.2007.616

Ortega Espluga, L., Poulliat, C., Boucheret, M.-L., Aubault, M., & Al Bitar, H. (2018a). Co-design of message structure and channel coding scheme to reduce the time to CED and to improve the resilience for a Galileo 2nd generation new signal. In *Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018)*, pp. 4064-4078. https://doi.org/10.33012/2018.15878

Ortega Espluga, L., Poulliat, C., Boucheret, M.-L., Aubault, M., & Al Bitar, H. (2018b). New solutions to reduce the time-to-CED and to improve the CED robustness of the Galileo I/NAV message. In *ION Position Location and Navigation Symposium (ION Plans 2018)*, pp. 1399–1408. https://doi.org/10.1109/PLANS.2018.8373532

OS SIS ICD. (2016). *Galileo – Open service signal in space interface control document (OS SIS ICD V1.3)*. European Union.

Prieto-Cerdeira, R., Perez-Fontan, F., Burzigotti, P., Bolea-Alamañac, A., & Sanchez-Lago, I. (2010). Versatile two-state land mobile satellite channel model with first application to DVB-SH analysis. *International Journal of Satellite Communications and Networking*, 28(5–6), 291–315. https://doi.org/10.1002/sat.964

Roudier, M. (2015). *Analysis and improvement of GNSS navigation message demodulation performance in urban environments* (PhD thesis). INP Toulouse. Retrieved from http://ethesis.inp-toulouse.fr/archive/00003004/

Ryan, W., & Lin, S. (2009). *Channel codes: Classical and modern*. New York: Cambridge University Press. https://doi.org/10.1017/CBO9780511803253

Schotsch, B. E., Anghileri, M., Burger, T., & Ouedraogo, M. (2017). Joint time-to-CED reduction and improvement of CED robustness in the Galileo I/NAV message. In *Proceedings of the 30th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2017)*, pp. 1544–1558. https://doi.org/10.33012/2017.15374

Thorpe, J. (2003). Low-density parity-check (LDPC) codes constructed from protographs. *IPN Progress Report*, 42(154), 42–154. Retrieved from https://ipnpr.jpl.nasa.gov/progress_report/42-154/154C.pdf

Uchôa, A. G. D., Healy, C., Lamare, R. C., & Souza, R. D. (2011). Design of LDPC codes based on progressive edge growth techniques for block fading channels. *IEEE Communications Letters*, 15(11), 1221–1223. https://doi.org/10.1109/LCOMM.2011.092911.111520

Viterbi, A. J. (1967). Error bounds for convolutional codes and an asymptotically optimum decoding algorithm. *IEEE Transactions on Information Theory*, 13, 260–269. https://doi.org/10.1109/TIT.1967.1054010

APPENDIX: ERASURE-DECODING ALGORITHM
Here, the low-complexity erasure algorithm (Blaum & Roth, 1999), used by the LD-MDS code scheme to retrieve the systematic information once k error-free information units have been supplied, is presented. From the parity check matrix defined in Equation (10), the syndrome vector of the received messages $(Z_l)_{k+2}^{l=1}$ over $GF(2^{p-1})$ are defined by:

$$S_0 = Z_1 + Z_2 + \cdots + Z_k + Z_{k+1} \qquad \text{(A1)}$$

$$S_1 = \beta_1 Z_1 + \beta_2 Z_2 + \cdots + \beta_k Z_k + Z_{k+2}, \qquad \text{(A2)}$$

where $(Z_l)_{k+2}^{l=1}$ denote the vector which represents the received word $(Z_l)_{k+2}^{l=1}$.

Now assume that the received words $(Z_l)_{k+2}^{l=1}$ have been erased at the entries i and j, $1 \le i < j \le k+2$. As Z_i and Z_j are erased, we initially set $Z_j = Z_i = 0$. We have three possible options:

- It is clear that if $j = k+2$, the error $e_i = S_0$;
- if $j = k+1$, the error $S_0 = e_i + e_{k+1}$ and $S_1 = \beta_i e_i$; so,

$e_i = \beta_i^{-1} S_1$ and $e_{k+1} = S_0 - \beta_i^{-1} S_1$;
- if $1 \le i < j \le k$, then $S_0 = e_i + e_j$ and $S_1 = \beta_i e_i + \beta_j e_j$; this yields $e_j = (\beta_j - \beta_i)^{-1}(S_1 - \beta_i S_0)$ and $e_i = S_0 - e_j$.

From the identities above, we develop the next algorithm:

- Set $Z_j = Z_i = 0$
- if $j = k+1 \rightarrow Z_{k+1} = -(S_1 - \beta_i^{-1} S_0) =$
- else if $1 \le j \le k \rightarrow Z_j = -(\beta_j - \beta_i)^{-1}(S_1 - \beta_i S_0)$.

Let $Z_i = -(S_0 + Z_j)$, and the algorithm output is the data allocated in the vectors $(Z_l)_k^{l=1}$.