New Solutions to Reduce the Time-To-CED and to Improve the CED Robustness of the Galileo I/NAV Message

Lorenzo Ortega Espluga
TéSA
Toulouse, France
lorenzo.ortega@tesa.prd.fr

Charly Poulliat,Marie-Laure Boucheret
INPT
Toulouse, France

Marion Aubault
CNES
Toulouse, France

Hanaa Al bitar
Thales Alenia Space
Toulouse, France

***Abstract*— In the current framework of Galileo and thanks to the flexibility of the I/NAV message, introducing new pages in order to propose an optimization of the E1-B Galileo signal has been proposed [1]. This optimization process pursues two different objectives. The first objective aims to reduce the Time To First Fix (TTFF), achieved by shortening the time to retrieve the Clock and Ephemerides Data (CED). The second objective aims to improve the resilience and robustness of the CED, particularly under hostile environments.**

Under the backward compatibility precondition, new outer channel error correction solutions for Galileo I/NAV are proposed in this paper. Especially, a new family of codes called Lowest Density Maximum Distance Separable codes (LD-MDS) is proposed to be used in this paper, thus in GNSS context. This family of codes, along with an enhanced performance decoding method based on the use of a soft serial iterative decoding, provides an optimal solution in order to reduce the TTFF as well as to improve the robustness of the CED.

Keywords—Galileo; low-density codes; MDS codes; soft serial iterative decoding; clock and ephemerides data; time to first fix.

I. INTRODUCTION

Within the framework of Galileo and more precisely inside the European GNSS OS SIS ICD publication [2], the proposed Galileo I/NAV message provides the flexibility to introduce new pages types. These new pages can be used to propose an optimization of the Galileo I/NAV message on E1-B to meet the following objectives: under the precondition to keep the backward compatibility with the current I/NAV message structure, the first objective is a reduction of the Time To First Fix (TTFF) achieved by reducing the time to retrieve the complete Clock and Ephemerides Data (CED), so-called Time To Data (TTD), and the second objective consists in improving the CED robustness, especially in difficult environments.

In order to meet these objectives, this paper proposes optimized backward compatible error correcting solutions to both reduce the TTD and improve the robustness of the CED. To this aim, an outer channel coding scheme [1] is proposed to be added to the baseline coding scheme of the Galileo I/NAV messages based on a convolutional code (for error correction) and CRC (Cyclic Redundancy Check) for error detection. Introduction of this new outer coding scheme is possible when considering the use of some new (unused so far) additional pages than can carry the extra redundancy introduced by this outer coding scheme.

After presenting the proposed new scheme and the structure of the message, a new category of codes, referred to as Lowest Density Maximum Distance Separable codes (LD-MDS) [4], is thus proposed for this outer coding scheme. These codes were first presented in the area of the multiple disk array applications and then routed to the fast distributed storage systems. They are well known for supply High Speed (HS) encoding and decoding as well as to tolerate multiple disk failure.

The new error and erasure correcting scheme is then presented for hostile GNSS environments and is compared with some reference error correcting schemes, presented in the state of the art [1], that will use both standard irregular Low Density Parity Check (LDPC) [6] codes and Reed Solomon (RS) codes [7] as outer coding schemes.

The proposed family of codes combines two properties:

- The first property is the Maximum Distance Separable (MDS) property as it exists for RS codes. Thanks to this property, the time to retrieve the CED can be reduced.
- The second property derives from the sparse structure of the parity check matrix, which can be considered as the lowest density parity check matrix, having the MDS property. This enables the use of low-complexity iterative erasure decoding algorithms and allows for the serial iterative soft detection in combination with the inner legacy convolutional code of the Galileo I/NAV message.

The paper is organized as follows. Section II reviews the current Galileo I/NAV message structure on E1-B and presents the inner coding scheme based on convolutional codes. We further assess in this section how extra redundancy can be introduced based on the use of an outer coding scheme. Section III presents the LD-MDS codes namely proposed as an outer coding scheme. We also present how this new type of codes can be efficiently used within a soft iterative decoding scheme enabled by the serially concatenated scheme composed of the outer and the inner coding schemes. Section IV presents two

error correcting solutions from the state of the art [1], as well as two new error correcting solutions based on LD-MDS codes and the soft iterative decoding scheme. Their performance is presented and analyzed in Section V. Conclusions are finally drawn in Section VI.

II. GALILEO I/NAV MESSAGE FOR E1-B SIGNAL AND THE PROPOSED OUTER CODING SCHEME

The navigation message is an essential part in the GNSS signals. Amongst others, this navigation message mainly provides the user with all the data needed to compute Position-Velocity-Time (PVT) solution. In some cases, navigation messages include additional resources in order to provide supplementary services.

In this paper, we focus on the I/NAV message, which contains the CED of the E1-B signal. In Figure 1, the I/NAV nominal page structure is illustrated. Inside each page, 2 subpages are included: the even subpage, which stores 16 bits of data besides other state information such as the CRC bits, and the odd subpage, which includes 112 bits of data. The total 128 bits of data are equivalent to one word of information, with the first 6 bits representing the word type.

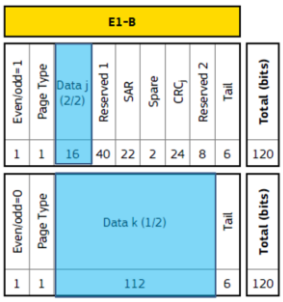

Fig. 1. I/NAV E1-B Nominal Page with Bits Allocation [2]

Each subpage has 120 bits, which are encoded by a rate one-half convolutional code with polynomial generators in octal representation given by (171,133). At the output of the convolutional encoder, 240 data symbols are interleaved by a 30x8 block-interleaver. Finally, 10 bits of synchronization are added at the beginning of the data frame. Figure 2 shows the flow diagram of the described process.

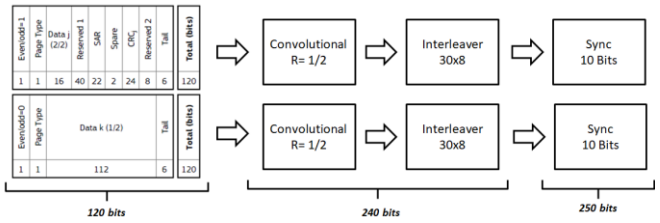

Fig. 2. Flow-Diagram of I/NAV Data Generation

The composition of 15 nominal pages, each one with a duration of 2 seconds, represents the 30 seconds duration of the I/NAV E1-B subframe structure [2], illustrated in figure 3. Within the subframe structure, pages 1, 2, 11 and 12 are used to store the 4 CED information words. Therefore, every 30 seconds, 4 CED information words, which are equivalent to 4x122=488 bits CED data bits, are provided by the I/NAV message.

Some pages within this 30 seconds frame are not used yet. Thus, introducing a new outer coding scheme is possible considering these unused pages that can carry extra redundant data. In the current proposed outer coding scheme, pages 8 and 9 have been selected to store the redundant data generated by the extra outer coding channel method, considered as Forward Error Correction 2 (FEC2). In other words, two extra pages, equivalent to 244 data bits, are available to store redundant data generated by the outer coding channel method. With these considerations in mind, a general outer channel coding (n, k) 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 with the existing message, systematic channel coding is mandatory. As a consequence, in the proposed outer coding channel method, systematic information bits are stored in pages 1, 2, 11 and 12 while redundant bits are stored in pages 8 and 9.

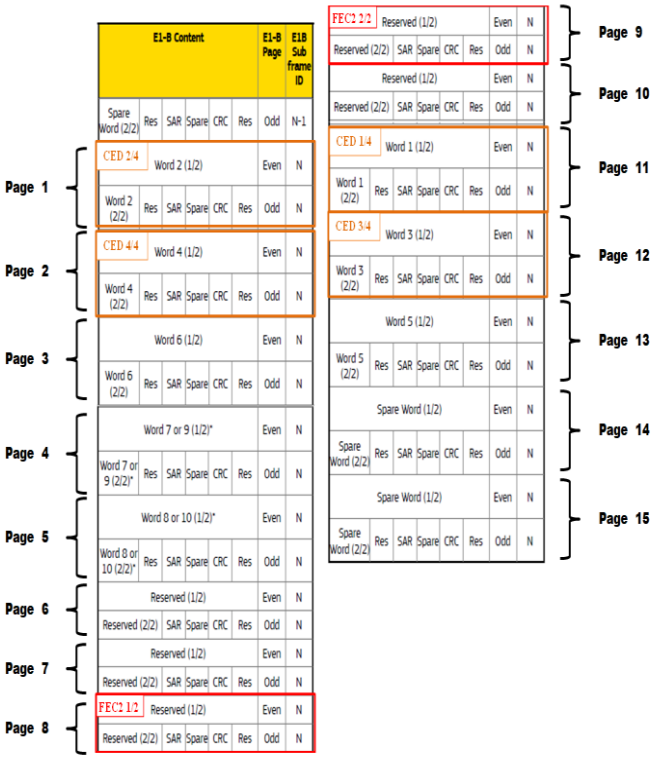

Fig. 3. I/NAV E1-B Nominal Sub-frame Structure [1]

III. LD-MDS CODES & SOFT SERIAL ITERATIVE DECODING

In this section, the materials for the definition of the proposed new error correcting methods of Section III are presented. First, we review the method to generate LD-MDS codes as well as the analytical expressions. Then, the soft serially concatenated iterative scheme is presented. This scheme describes the decoding process between the Soft Input Soft Output (SISO) decoder of the mandatory inner

convolutional code (i.e. bitwise Maximum A Posteriori (MAP) based on the BCJR algorithm [3] [9]) and the outer SISO decoder of the LD-MDS and LDPC codes which finally reduces to the well-known Belief Propagation (BP) decoding algorithm.

A. Lowest Density Maximum Distance Separable Codes

A new category of possible codes referred as LD-MDS codes [4] is presented in the following section. Those codes combine two main properties. The first property is the Maximum Distance Separable (MDS) property, which allows retrieve k data units of systematic information from any k free error information units (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. Moreover, under the backward compatibility constraint, systematic channel coding solutions are required.

B. Definition of MDS Codes

Let C be a code of length n over $GF(q^b)$ with b a positive integer and let C have the minimum Hamming distance d, where the distance is measured with respect to symbols of $GF(q^b)$. By the Singleton bound for codes over $GF(q^b)$, the codes that attain the following bound are called MDS [4] codes:

$$d \leq n + 1 - k \tag{1}$$

where $k = log_q{}^b/C/$ is an information symbol length, n is the length of the codeword over $GF(q^b)$ and $r = n - k$ is the check symbol length. An example of such as codes are the RS codes over $GF(q^b)$. It is interesting to emphasize that each symbol over $GF(q^b)$can be interpreted as block of length b over $GF(q)$ and as consequences the set of codewords define a code of length nb Let T be a kb x rb matrix over $GF(q)$ the systematic generator and parity check matrices are defined in (2) and (3):

$$G = [I \quad T] \tag{2}$$

$$H = [T^T \quad I] \tag{3}$$

where I is the identity matrix, G is a kb x nb matrix and H is rb x nb matrix.

C. Construction of MDS Codes over

[4] presents the construction of linear $[k+2,k]$ MDS codes over $GF(q^b)$ whose systematic parity check and generator matrices are defined in as in equations (4) and (5).

$$H_\beta = \begin{pmatrix} I & I & I & \cdots & I & I & 0 \\ \beta_1 & \beta_2 & \beta_3 & \cdots & \beta_k & 0 & I \end{pmatrix} \tag{4}$$

$$G_\beta = \begin{pmatrix} I & 0 & 0 & \cdots & 0 & -I & -\beta^T{}_1 \\ 0 & I & 0 & \cdots & 0 & -I & -\beta^T{}_2 \\ 0 & 0 & I & \cdots & 0 & -I & -\beta^T{}_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & I & -I & -\beta^T{}_k \end{pmatrix} \tag{5}$$

where $\beta=\{\beta_1,\beta_2,\ldots,\beta_k\}$ is a set of b x b matrices over $GF(q)$. In order to construct a MDS code, the set 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 1s in the parity check matrix, the lower complexity in the coding and decoding algorithms. As a consequence we fix the following property:

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

Let us first define a binary system with $q=2$. To generate a subset of matrices β we must first construct a set of matrices which satisfies (P1)-(P3) [5], we denote such as set of matrices as Q_α^i. The set of matrices Q_α^i are obtained from definition 1:

1) Definition 1

Let p as an odd prime and α as an element of $GF(q)$-$\{0\}$. (In our case as $q=2$, $\alpha=1$). For $0 \leq i \leq p$, we define the b x b = $(p-1)$x$(p-1)$ matrix $Q_\alpha^i = v_{l,m}$ where $l,m \in (1,p-1)$ over $GF(q)$ where $v_{l,m}$ is defined in equation (6). We can redefine the parameters for $q=2$, $\alpha=1$, obtaining the following subset of b x b matrix $Q_\alpha^i = v_{l,m}$ where $l,m \in (1,b)$ over GF(2). $v_{l,m}$ for the new parameters is defined in equation (7).

$$v_{l,m} = \begin{cases} 1 & if\ l \neq p-i\ and\ (m-l)mod(p) = i \\ -1 & if\ l = p-i\ and\ (m-l)mod(p) = i \\ -\alpha & if\ l = p-i\ and\ m = \langle i/2 \rangle \\ 0 & otherwise \end{cases} \tag{6}$$

$$v_{l,m} = \begin{cases} 1 & if\ l \neq p-i\ and\ (m-l)mod(p) = i \\ 1 & if\ l = p-i\ and\ (m-l)mod(p) = i \\ 1 & if\ l = p-i\ and\ m = \langle i/2 \rangle \\ 0 & otherwise \end{cases} \tag{7}$$

where the operation $\langle a/b \rangle$ denote the integer between $0 \leq \theta \leq p$, such that $a \equiv b\theta(mod\ p)$.

In order to generate MDS codes (ie. to obtain the subset of matrices β), the subset of matrices Q_α^i must fulfill (P2). In order to satisfy (P2), theorem 2.6 [5] provides sufficient conditions on p and α so that Q_α^i satisfies (P2). Once the subset of matrices Q_α^i satisfies (P1)-(P2) and (P3), the set of matrices β is created by selecting a subset of the set defined by Q_α^i matrices.

D. LD-MDS Codes as LDPC

Previously, the LD-MDS codes were defined by having a parity check matrix H with the fewer 1's. Such as sparsity in the parity check matrix enables to introduce the decoding algorithm used by the LDPC codes (BP algorithm). In other words, LD-MDS codes can be viewed as LDPC codes with the MDS property. Moreover, thanks to sparse parity check matrix and the MDS property, a low complexity erasure decoding algorithm can be developed for LD-MDS codes. The erasure decoding algorithm is presented in ANNEX A.

E. Soft Serial Iterative Decoding

A soft serial iterative decoding between the SISO decoder of the mandatory inner convolutional code and the SISO decoder of the outer channel coding (LDPC Decoder), has been proposed in order to improve the resilience of the clock and ephemeris data and to reduce the TTD in bad channel environment for some of the schemes presented in Section III. The soft serial iterative decoding method improves the performance of the well-known belief propagation decoding algorithm by introducing a more elaborate decoding algorithm. Figure 4 illustrates the generic soft serial iterative decoding scheme [3].

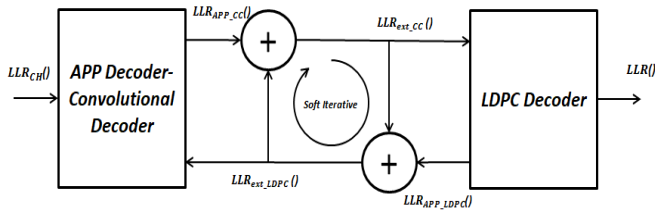

Fig. 4. Soft Serial Iterative Decoding

Instead of using the default Viterbi algorithm to decode the convolutional data to perform Maximum Likelihood (ML) sequence estimation, we will rather consider Maximum A Posteriori (MAP) symbol detection in order to enable soft iterative decoding between the LDPC decoder and the SISO MAP decoder associated with the convolutional code. We will consider soft decoding algorithms exchanging soft information carried out by Log-Likelihood Ratios (LLR), as defined by equation (8) with some abuse of notations.

$$LLR(u) = \log\left(\frac{p(u=0)}{p(u=1)}\right) \tag{8}$$

The overall iterative decoding procedure can be summarized as follows. First, LLR derived from the demodulator are provided to the convolutional A Posterior Probability (APP) decoder [3] based on the BCJR algorithm or one of its low-complexity versions. Moreover, in an iterative process, the APP decoder can also benefit from the a priori information provided by the LDPC decoder. Using this information, the APP decoder outputs some soft information that is fed to the soft LDPC decoder. After executing one or several iterations of the Belief Propagation (BP) algorithm, which is the low complexity soft decoding algorithm used to decode LDPC codes, soft information output by the BP decoder are fed back as a priori to the convolutional APP decoder. Applying the preceding operations iteratively allows for an improvement on the final system performance.

We now review in details the messages exchanged by both soft decoders. Let the extrinsic Log-Likelihood ratio LLR_{ext} be defined as the extrinsic information exchanged between soft decoding modules during the iterative decoding process. It is usually obtained from a posteriori LLRs, given by a soft decoding module, by removing the a priori information given by the other soft decoding module as given in Figure 4. The soft serial iterative decoding is described as follows:

- For one global iteration, *LLRs* provided by the soft demodulator LLR_{CH} and a priori information LLR_{ext_LDPC} are used as inputs of the symbol MAP APP Decoder. Then, soft APP decoding of the inner convolutional code is performed. The output is given by the vector LLR_{APP_CC}. After removing the a priori information given by LLR_{ext_CC} information, LLR_{ext_CC} is provided as an input to the soft input LDPC Decoder.

- Then soft LDPC decoding is performed for one or several iterations and outputs LLR_{APP_LDPC}. After removing the a priori information LLR_{ext_CC}, LLR_{ext_LDPC} is provided as a priori information to the soft APP decoder of the inner convolutional code. Note that for the first iteration, LLR_{ext_LDPC} is a vector of zeros, which is equivalent to assuming that no a priori information on information bits is available from the outer LDPC decoder.

IV. Error Correcting Solutions

In this paper, four error correcting solutions (two from the state of the art [1] and two new solutions), working as an additional outer channel coding scheme to the baseline coding scheme of the Galileo I/NAV message, have been studied. Those error correcting solutions along with their specific characteristic are described in table 1.

TABLE I. Error Correcting Solutions Parameters

Error Correcting Solution	Characteristics
Convolutional + Reed Solomon no serial iterative decoding (already proposed in [1])	Convolutional decoder: • SIHO Viterbi decoder [6] Erasure and error correcting: • Berlekamp-Massey decoding algorithm [8]
Convolutional + LDPC no soft serial iterative decoding (already proposed in [1])	Convolutional decoder: • SISO APP decoder, BCJR algorithm [9] LDPC decoder: • SISO BP decoder [7] • Number of LDPC iterations = 100
Convolutional + LDPC soft serial iterative algorithm (new solution)	Convolutional decoder: • SISO APP decoder, true APP LDPC decoder: • SISO BP decoder • Number of internal LDPC iterations = 1 Number of soft serial iterations = 100
Convolutional + LD-MDS soft serial iterative	Error correcting algorithm: • Convolutional decoder:

algorithm (new solution)	• SISO APP decoder, BCJR algorithm
	• LDPC decoder:
	  ○ SISO BP decoder
	  ○ Number of internal LDPC iterations = 1
	• Number of soft serial iterations = 100
	Erasure algorithm [4]
	• Low complexity erasure LD-MDS algorithm

A. *Convolutional + Reed Solomon*

The Reed Solomon scheme, viewed as an additional outer coding scheme to the current I/NAV scheme, was already proposed in [1]. The RS codes provide erasure and error correction capabilities. Those capabilities bring benefits to users that are receiving signals in both good and bad channel conditions. If the channel is good, the user can take advantages of the MDS property to retrieve the k CED blocks as soon as possible. To recover k CED blocks, k free-error blocks are required (data information or redundant information). In order to identify if the data blocks are free of errors, the CRC data provided by the I/NAV message is used.

Under hostile environment when both erasure and errors occur; the RS correction capability can be used in order to retrieve the information data.

Both erasure and error correcting RS algorithms do not need soft input information. Consequently, a Soft Input Hard Output (SIHO) algorithm, such as the Viterbi algorithm, provides a low complex decoding solution to decode the convolutional information.

B. *Convolutional + LDPC No Serial Iterative Decoding*

LDPC codes were already proposed in [1], as an additional outer coding scheme to the current I/NAV scheme. In this work, the following scheme has been proposed. The *4x122* (see section I) CED bits are encoded by a LDPC systematic code *(n,k)* where *n=728* and *k=488*. Encoded information is stored in the pages 1, 2, 8, 9, 11 and 12, following the backward compatibility requirement. The convolutional encoder *(171,133)* with a rate ½ as well as the block interleaver *(30x8)* provided by the current I/NAV system are introduced. Finally, 10 synchronization bits are added at the beginning of the each subpage. Figure 5 illustrates the encoding diagram flow described above.

Several possible solutions can be selected in order to provide a convolutional decoder. For instances, the current system uses a SIHO Viterbi decoder. In the current proposition, since BP algorithm used by the LPDC decoder needs a soft input, a convolutional Soft Input Soft Output (SISO) decoding algorithm is required. One of the most common convolutional SISO decoding algorithms is the APP decoder [3] [7], which has been selected as the convolutional soft decoder.

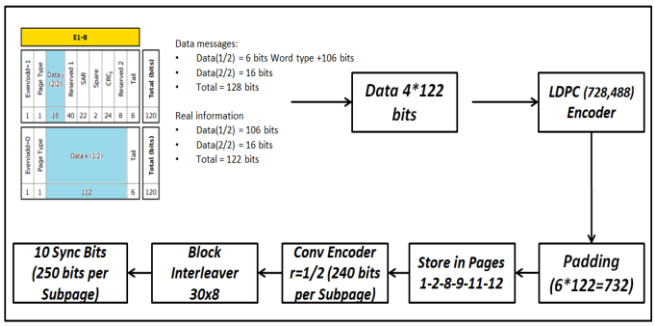

Fig. 5. LDPC + Convolutional Encoding Scheme

To exploit the presence of the LDPC parity words, the Galileo receiver shall process the incoming message. Both CED data words (pages 1-2-11-12) and LDPC data words (pages 8-9) shall be stored in a buffer. In case of retrieving 4 error-free CED data words, CED data would have been retrieved, otherwise as soon as 4 CED words and 2 LDPC words were collected, the BP-LDPC error correction algorithm could be executed. In case of error decoding, the receiver needs to wait for the reception of new CED or LDPC words. Reception diagram flow is illustrated in figure 8.

In order to check if the incoming words bring reliable information, a CRC computation is needed. Once the CRC has been computed, those bits are compared with the received CRC bits. On the other hand, in case of executing the LDPC decoding algorithm, the parity check matrix can be also used as an error detection method.

C. *Convolutional + LDPC Soft Serial Iteration Algorithm*

In order to enhance performance at the decoding stage, the soft serial iterative algorithm presented in Section III is proposed as error decoding solution. In this scheme, the soft information provided by the demodulator is used by the APP decoder algorithm as an input. Moreover, the APP decoding algorithm benefits from the a-priori information provided after the BP algorithm.

The number of serial iterations has a direct effect in both complexity and retrieved CED error probability performance; therefore a higher number of iterations provides outstanding results in terms of CED error probability but also increase the number of operations and the decoding latency as well.

The decoding diagram flow is illustrated in Figure 6 and the reception diagram flow is illustrated in figure 7.

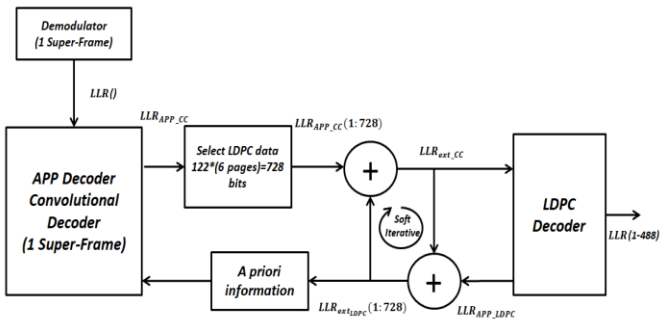

Fig. 6. Error Serial Soft Iterative Decoding Algorithm

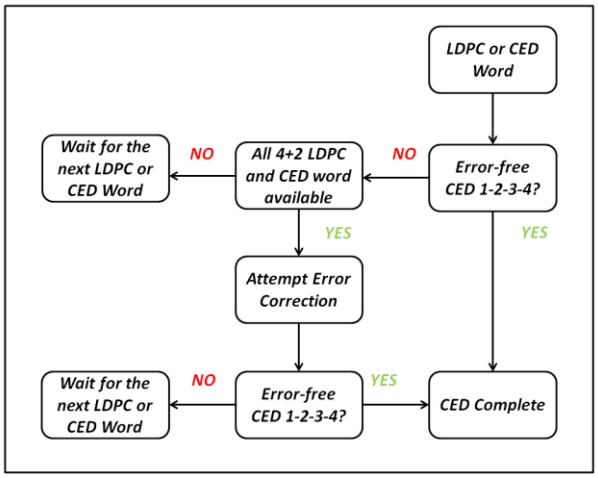

Fig. 7. Convolutional + LDPC Decoding Process

D. *Convolutional + LD-MDS Soft Serial Iterative Decoding Algorithm*

LD-MDS codes are proposed as an additional outer coding scheme to the current I/NAV scheme. Those codes were introduced in Section III. System parameters are defined as: $n = 6$, $k = 4$ and $q = 2$. The CED data block is equal to *122* bits. In order to obtain the b value:

- Select $b = 122 \rightarrow p = b + 1 = 123$, p equal to odd prime is not accomplished.
- Split b in two possible blocks $b1$ and $b2$ following the next constraints:
  - $b1 + b2 = 122$
  - $p1 = b1 + 1$ is an odd prime
  - $p2 = b2 + 1$ is an odd prime

Table 2 presents the possible combination for b1 and b2.

TABLE II. ERROR CORRECTING SOLUTIONS PARAMETERS

	b1	***b2***
Option 1	106	16
Option 2	82	40
Option 3	70	52

Figure 8 illustrates the data encoding process. The systematic data blocks are split into two parts equivalent to $b1$ bits and $b2$ bits respectively. Each subset of k blocks is encoded by the LD-MDS generator matrix. After the encoding stage n blocks of $b1$ and $b2$ bits are stored in pages 1-2-8-9-11-12. The legacy convolutional encoder is used to encode the systematic part.

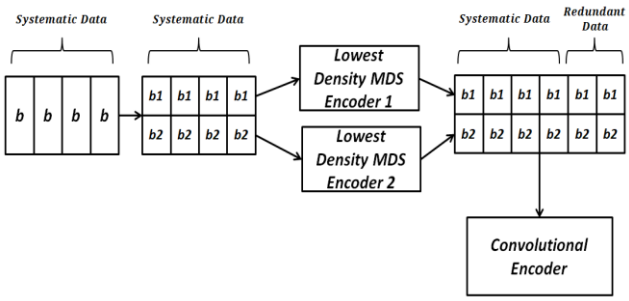

Fig. 8. LD-MDS Encoder with Convolutional Encoder

In order to decode the data information two algorithms are applied. In case of error after retrieving the APP decoder data information, the serial soft iterative decoding algorithm illustrated in figure 6 is executed. In case of 4 free error data information blocks, a low complexity erasure LD-MDS algorithm, which is presented in Annex A, is used to retrieve the CED information. Free error blocks are detected thanks to the CRC error detection technique provided by the current I/NAV Galileo framework. Figure 9 illustrates the block diagram used by the LD-MDS decoding scheme.

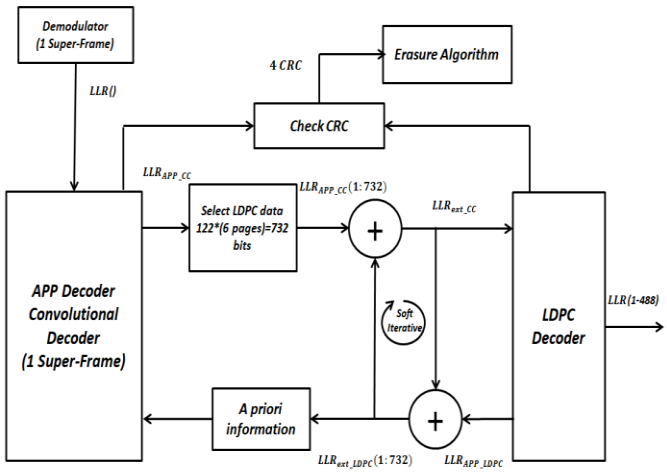

Fig. 9. Lowest Density MDS Codes Decoder + Convolutional Decoder Block Diagram

Figure 10 illustrates the flow diagram of the LD-MDS decoding process. The Galileo receiver shall process the incoming messages. In order to retrieve the CED information, at least 4 free errors words (information or redundant words) are required. In that case, the erasure correction algorithm (low complexity erasure LD-MDS algorithm) can be applied to retrieve the CED information. If at least one of these 4 words is incorrect, the error correcting method can be executed in order to correct and recover the corrupted bits. In case of the error correcting method will not be capable to retrieve the CED information; a new incoming information word has to be awaited.

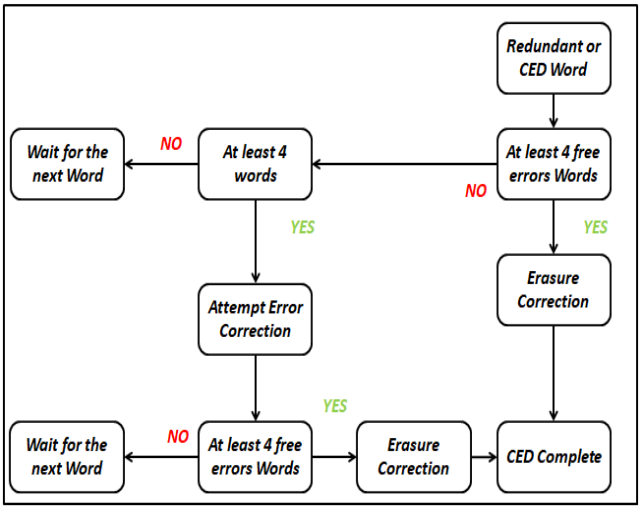

Fig. 10. Convolutional + LD-MDS Codes Decoding Process

V. Error Correcting Solutions

In order to compare the performances of the 4 error correcting solutions proposed in the Section IV, retrieved CED Error Rate (CEDER) and the TTFF are evaluated. In table 2, the error correcting proposed solutions as well as their simulation parameters are described.

A. Retrieved CED Error Probability

The Additive White Gaussian Noise (AWGN) channel is the model used to estimate the background noise on the transmission channel. This model does not include fading or interferences coming from other sources. The model follows the equation 9 [10]:

$$y_k = x_k + n_k \tag{9}$$

where y_k is the received signal, x_k is the transmitted signal and n_k is the AWGN sample. Moreover $n_k \sim N(0,\theta^2)$ where $\theta^2 = N_0/(4T_i)$[10] and T_i = 4ms.

For our performance evaluation, we assume that the entire subframe has been received, in other words when the 6 information units (4 CED and 2 redundant data words) have been received. Figure 11 illustrates the CED error probability in terms of C/N0 for the error correcting solutions described in section IV as well as for the baseline Galileo coding scheme.. Furthermore, in case of the LD-MDS scheme, the three configurations proposed in section IV-D have been tested.

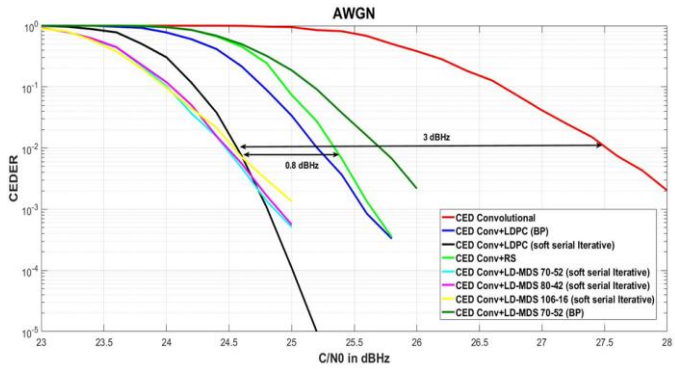

Fig. 11. CED recovery error probability when a subframe (30s) is retrieved over AWGN channel

Retrieved CED Error Rate (CEDER) simulations are illustrated in Figure 11. Simulations show that using a more robust decoding scheme, such as soft serial iterative decoding involves an increase of the robustness over the CED. Therefore, the proposed decoding schemes LDPC soft serial iterative decoding and LD-MDS soft serial iterative decoding enhance the performance showed by the state of the art (LDPC BP decoding and RS decoding). As it was done in [1], the error correcting algorithms for each new proposed scheme will be evaluated and compared for a targeted error probability of 10^{-2}. Results further show that the soft serial iterative decoding algorithm gives an improvement of 0.7 dBHz with respect to the basic Soft Input BP algorithm used by the LDPC decoder and an overcome of the performances bigger than 0.8 dBHz with respect to the Hard Input Berlekamp-Massey decoding algorithm used by the Reed Solomon decoder, while ensuring a demodulation threshold gain of 3 dB compared with the current I/NAV message (in red line).

B. Time To Data (TTD)

In order to evaluate the TTD, it is required to define the TTFF [2] which is referred to as the time needed by the receiver to perform the first position fix. The expression is given as follows:

$$T_{TTFF} = T_{warm\ up} + T_{tracking} + T_{acquistion} + T_{TTD\ data} + T_{PVT} \tag{10}$$

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 average, 95 % and worst-case time values.

To obtain the average and 95% time values [11], we need to define the Probability Density Function (PDF) *f(t)* of the TTD. The average and 95% probability can then be obtained from the

Cumulative Distribution Function (CDF) defined in equation 12.

$$F(T_{CED}) = \int_{-\infty}^{T_{CED}} f(t)dt = x \tag{11}$$

where $x = 0.5$ to obtain the average time value and $x = 0.95$ to obtain the time value which represents the time needed by the receiver to retrieve CED with the 95% confidence.

For simulations, 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 under C/N0=25 dBHz and C/N0=45 dBHz. As expected, the first epoch (first synchronized bit) can arrive at any time. Following the structure of I/NAV message, each subframe represents 7500 bits, therefore in order to initialize the first epoch value for each of the 100.000 simulations, an uniform distribution with values between 1 and 7500 is used. Each of the values represents a possible first synchronized bit.

In order to reduce the complexity of the simulation and to illustrate the impact of the error correction algorithms showed in Figure 11, the error correcting algorithms are run once the 6 information blocks (4 CED + 2 redundant information) have been received. This simulation mode differs from the real algorithm implementation, where the error correcting capability is available once 5 information blocks have been received in case of RS codes or 4 information blocks for LD-MDS codes.

CDF for the 4 error correcting solutions as well as the baseline Galileo solution using the parameters defined above are presented in Figure 12 and Figure 13. Moreover, tables 3 and 4 represent the average and the 95 % and worst-case time values for each of the candidate solutions.

From the tables and the figures, it can be seen that under good conditions (C/N0=45 dBHz), RS and LD-MDS solutions are able to reduce the TTD thanks to both the MDS property, which allows a user to retrieve the CED as soon as 4 error free information units are available, and to the availability of erasure decoding algorithms which are able to make use of such MDS property. In the case of LDPC codes, whatever the error correcting algorithm used, the 4 CED error free information units are needed in order to retrieve the whole CED frame. As a consequence, under good channel conditions, LDPC codes keep the same time performances as the current Galileo I/NAV message.

Under bad channel conditions (C/N0=25 dBHz), a lower CED error probability provides a reduction in the time to retrieve the CED. As it was illustrated in Figure 11, serial soft iterative algorithms provide a lower error probability than the BP or the Hard Input Berlekamp-Massey decoding algorithms, therefore LD-MDS and LDPC codes under the serial soft iterative algorithm overcome the TTD performances to RS codes or LDPC codes with the BP decoding algorithm. It must be pointed out that serial soft iterative algorithm increases the complexity of the decoding algorithm.

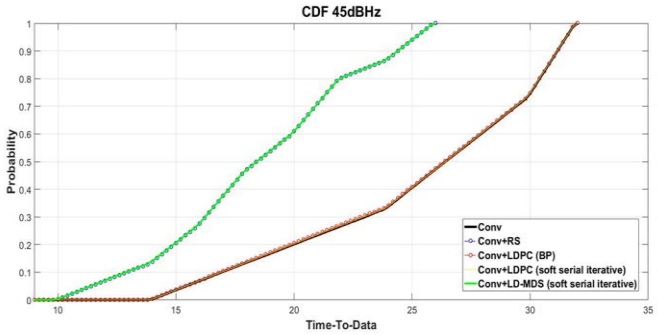

Fig. 12. CDF of the Error Correcting Candidates C/N_0 = 45 dBHz

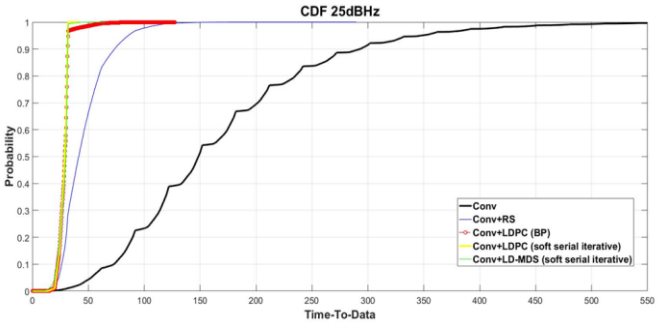

Fig. 13. CDF of the Error Correcting Candidates C/N_0 = 25 dBHz

TABLE III. TTD 50% CONFIDENCE

TTD 50% confidence	**25 dBHz**	**45 dBHz**
Current Galileo I/NAV	148.4 seconds	26.6 seconds
RS	41.4 seconds	18.4 seconds
LDPC BP	29 seconds	26.6 seconds
LDPC serial soft iterative	28.8 seconds	26.6 seconds
LD-MDS serial soft iterative	30 seconds	18.4 seconds

TABLE IV. TTD 95% CONFIDENCE

TTD 95% confidence	**25 dBHz**	**45 dBHz**
Current Galileo I/NAV	347.8 seconds	31.6 seconds
RS	85.8 seconds	25.2 seconds
LDPC BP	32 seconds	31.6 seconds
LDPC serial soft iterative	31.8 seconds	31.6 seconds
LD-MDS serial soft iterative	31.8 seconds	25.2 seconds

In Section II, pages 8 and 9 were selected to store the redundant data generated by the extra outer coding channel method. In Figure 14, a new configuration where pages 6 and 7 are selected to store the redundant stored data is presented. This configuration is optimal under good channel conditions to retrieve CED with the 95% confidence since it reduces the maximum time to retrieve the CED. The results obtained with this configuration are depicted in the figure 14.

From former results, it can be concluded that combining the MDS property and the soft serial iterative decoding algorithm, as provided in the LD-MDS error correcting solution, an optimal joint time to CED reduction and improvement of the CED robustness is accomplished. Concerning the complexity of the receiver, the soft serial iterative decoding algorithm

complexity directly depends on the number of iteration needed to convergence. Therefore, the complexity of the algorithm depends on the channel conditions. A detailed research about the complexity is expected as work future line.

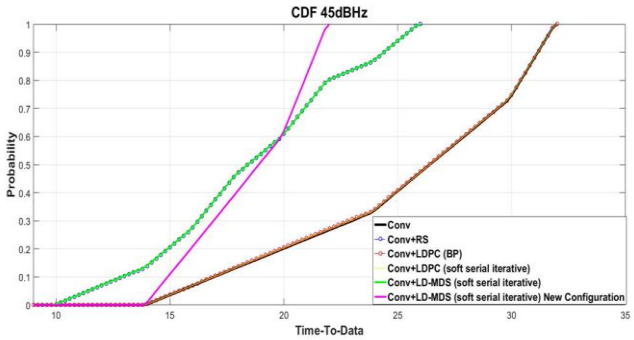

Fig. 14. CDF of the Error Correcting Candidates C/N_0 = 45 dBHz New Configuration

VI. Conclusion

This paper has proposed several new, though backward compatibility, error correcting solutions in order to optimize the Galileo I/NAV message for the E1-B signal. This optimization is achieved by the addition of an outer channel coding scheme to the coding scheme baseline (based on a convolutional code and a CRC error detection code) of the Galileo I/NAV message. Introduction of a new outer channel coding scheme is possible when considering the use of some (unused) additional pages than can carry the extra redundancy introduced by this outer coding scheme. The proposed error correcting solutions aim to fulfill two overarching objectives: the first goal is a reduction of the time to retrieve the complete CED and the second objective tackles the improvement of the CED demodulation robustness, particularly under hostile environments.

In this paper, a new category of codes, derived from disk arrays technology, referred to as LD-MDS are proposed as an erasure and error correcting scheme solution and is compared with some reference error correcting schemes that will use both standard irregular Low Density Parity Check (LDPC) codes and Reed Solomon codes as outer coding schemes. LD-MDS code family has the advantage of combining two properties: Maximum Distance Separable and sparse matrix.

The MDS property (also a characteristic of RS codes) allows to retrieve the CED through any *k* error free information pages of the total *n* information pages (whether nominal CED pages or redundant data pages) and as a consequence under good channel conditions (error free pages), the time to retrieve the first *k* information units (CED or redundant bits) will be the time to retrieve the CED.

On the other side, as well known, in order to reconstruct the CED from any *k* information units an erasure correction algorithm is then used. This is applicable to either with RS codes or LD-MDS codes. The main difference between both algorithms lies in the extremely low complexity of the LD-MDS erasure correction algorithm due to its sparse code structure.

The second property derives from the sparse structure of the parity check matrix. Sparse structure not only allows very efficient low complexity erasure correction algorithms, but also achievable message-passing error correcting algorithms. Moreover, in the case of stringent channel conditions, the underlying LDPC-like of LD-MDS code structure enables the use of soft serial iterative decoding between the mandatory inner convolutional code and the SISO decoder of the LD-MDS codes which finally is reduced to the well-known belief propagation decoding algorithm for LDPC codes [3]. Thus, an important gain on the demodulation threshold is obtained.

To sum up, the simulation results show that keeping the backward compatibility with the current I/NAV message, LD-MDS codes provide a new possible solution to reduce the TTD and finally the TTFF, and allow a demodulation threshold gain of 3 dB compared with the current I/NAV message. Moreover under good channel conditions, thanks to the low complexity erasure correcting algorithm, it is possible to retrieve the CED information with fewer operations than RS erasure correcting algorithm. Under bad channel conditions, and thanks to the use of low density parity check matrix, efficient error correcting algorithms can be used based on the soft serial iterative decoding scheme.

VII. ANNEX A

In this section, we explain the low complexity erasure algorithm [4], used by the LD-MDS code scheme, to retrieve the systematic information once k error free information units have been supplied. From the parity check matrix defined in (4), the syndrome values of the received messages $(Z_l), l \in (1,k+2)$ over $GF(2^{p-1})$ are defined by:

$$\underline{S}_0 = \underline{Z}_1 + \underline{Z}_2 + \cdots + \underline{Z}_k + \underline{Z}_{k+1} \tag{12}$$

$$\underline{S}_1 = B_1\underline{Z}_1 + B_2\underline{Z}_2 + \cdots + B_k\underline{Z}_{1k} + \underline{Z}_{k+2} \tag{13}$$

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

- It is clear that if $j=k+2$, the error $\underline{e}_i = \underline{S}_0$
- if $j=k+1$, the error $S_0 = \underline{e}_i + \underline{e}_{k+1}$ and $\underline{S}_1 = B_i\underline{e}_i$; so, $\underline{e}_i = B_i^{-1}\underline{S}_1$ and $\underline{e}_{k+1} = \underline{S}_0 - B_i^{-1}\underline{S}_1$
- if $1 \le i < j \le k$ then $\underline{S}_0 = \underline{e}_i + \underline{e}_j$ and $\underline{S}_1 = B_i\underline{e}_i + B_j\underline{e}_j$ thus yielding:
  - $\underline{e}_j = (B_j - B_i)^{-1}(\underline{S}_1 - B_i\underline{S}_0)$ and $\underline{e}_i = \underline{S}_0 - \underline{e}_j$

From the identities above we develop the next algorithm [4]:

- Set $\underline{Z}_j = \underline{Z}_i = 0$;
- If $j=k+1 \rightarrow \underline{Z}_{k+1} = -(\underline{S}_0 - B_i^{-1}\underline{S}_1)$
- Else if $1 \leq j \leq k \rightarrow \underline{Z}_j = (B_j - B_i)^{-1} (\underline{S}_1 - B_i\underline{S}_0)$

Let $\underline{Z}_i = -(\underline{S}_0 + \underline{Z}_j)$ and output $(Z_l), l \in (1,k)$

ACKNOWLEDGMENT

This work is funded by the French Space Agency, CNES, and Thales Alenia Space

REFERENCES

[1] Birgit E. Schotsch, Marco Anghileri, Thomas Burger, Mahamoudou Ouedraogo, “Joint Time-to-CED Reduction and Improvement of CED Robustness in the Galileo I/NAV Message”. "Proceedings of the 30th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2017), Portland, Oregon, September 2017.

[2] European GNSS (Galileo) Open Service - Signal-In-Space Interface Control Document, December 2016.

[3] WILLIAM E. RYAN, SHU LIN “Channel Codes: Classical and Modern”.

[4] BLAUM, M., AND ROTH, R. M. “On lowest density MDS codes”. IEEE Transactions on Information Theory 45, 1 (January 1999), 46-59.

[5] Eiji Fujiwara, “Code Design for Dependable Systems: Theory and Practical Application”, Wiley-Interscience, 2006 Chapter 3: Code Design Techniques for Matrix Codes.

[6] A. J Viterbi. "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm". IEEE Transactions on Information Theory vol. IT-13 pp. 260-269 April 1967.

[7] Gallager R.G, “Low-Density Parity-Check Codes, Cambridge”, MA, MIT Press, 1963.

[8] Reed, Irving S.; Solomon, Gustave (1960), "Polynomial Codes over Certain Finite Fields", Journal of the Society for Industrial and Applied Mathematics (SIAM), 8 (2): 300–304, doi:10.1137/0108018.

[9] L.Bahl, J.Cocke, F.Jelinek, and J.Raviv, "Optimal Decoding of Linear Codes for minimizing symbol error rate", IEEE Transactions on Information Theory, vol. IT-20(2), pp. 284-287, March 1974.

[10] Marion Roudier. “Analysis and Improvement of GNSS Navigation Message Demodulation Performance in Urban Environments”. PhD Manuscript, 2015.

[11] Paonni, Matteo, Anghileri, Marco, Wallner, Stefan, Avila-Rodriguez, Jose-Angel, Eissfeller, Bernd, "Performance Assessment of GNSS Signals in Terms of Time to First Fix for Cold, Warm and Hot Start," Proceedings of the 2010 International Technical Meeting of The Institute of Navigation, San Diego, CA, January 2010, pp. 1051-1066.