ORIGINAL ARTICLE

ION WILEY

High-parity vertical Reed-Solomon codes for long GNSS high-accuracy messages

Ignacio Fernández-Hernández[1] | **Tommaso Senni[2]** | **Daniele Borio[3]** | **Giovanni Vecchione[2]**

[1]DG for Defence Industry and Space, European Commission, Brussels, Belgium

[2]RHEA Group for European Commission, Brussels, Belgium

[3]Joint Research Centre (JRC), European Commission, Ispra, Italy

Correspondence
Ignacio Fernández-Hernández, DG for Defence Industry and Space, European Commission, BREY, Building 7/156, Avenue d'Auderghem 45, 1049 Brussels, Belgium.
Email: ignacio.fernandez-hernandez@ec.europa.eu

Abstract

This paper presents in detail an outer-coding proposal for long GNSS messages disseminated by multiple satellites. The proposal minimizes the message reception time, or Time To Retrieve Data (TTRD), over a page erasure channel in most types of environments and visibility conditions. A message $\mathbf{M}$ consisting of k pages is encoded into a set $\mathbf{C}$ consisting of n pages, such that when any subset $\mathbf{C}'$ of $\mathbf{C}$ of k pages is correctly received, the message can be decoded. The scheme vertically encodes each page symbol in a separate high-parity Reed-Solomon code and allocates different parts of it to different satellites. The scheme has been designed for the Galileo High Accuracy Service (HAS), but it can be used for longer messages and other constellations. The performance results show TTRDs on the order of few seconds, at a very low decoding complexity for the receiver.

1 | INTRODUCTION

Navigation satellites transmit their ephemerides and clocks in no more than a few hundred bits of their navigation message, allowing receivers to compute the satellite positions and, with them and the ranging measurements, their own position fix. However, there are some examples of satellite navigation messages that are much longer. For example, the satellite almanac requires twenty-four 30-second subframes, or 12.5 minutes, in the Galileo I/NAV message,[1] where each subframe transmits 256 bits of almanacs. Another example is the high-accuracy message of the Quasi-Zenith Satellite System's (QZSS) Centimeter-Level Augmentation Service (CLAS), where high-accuracy data is transmitted at a rate of 2000 bps and the message is generally structured in 30-second blocks.[2] Another example of long messages from Global Navigation Satellite System (GNSS) is the transmission of cryptographic information, starting with the Galileo Navigation Message Authentication (NMA), where over-the-air rekeying messages of more than a thousand bits will be regularly transmitted.[3] Other long messages include real-time ionospheric models or Long-Term Ephemeris (LTE). The Galileo Program will provide a High Accuracy Service (HAS) openly and freely, which also requires long messages. One of the challenges of GNSS is therefore ensuring a quick and reliable delivery of several-thousand-bit messages to all users, both in open-sky and degraded conditions. This paper proposes and studies an encoding and data dissemination scheme for such messages.

The main assumptions and figures of merit used in the rest of the work and the mathematical formulation of the problem are presented, along with a qualitative comparison of the main candidate coding schemes identified in the literature. Out of this comparison, Reed-Solomon codes,[4] and in particular high-redundancy vertical Reed-Solomon codes, provide a solution that is easy to implement and has the ideal property that when the number of received encoded pages equals the original number of pages, the message can be decoded.[5]

This coding scheme is described in detail in the next section and then particularized for the Galileo HAS, which is transmitted at a rate of 448 bps in the E6-B (1278.75 MHz) signal component, including the reception of two messages of 6360 and 848 bits, respectively. Next, the article presents the performance results of the proposed scheme in terms of Time To Retrieve Data (TTRD), including both theoretical Additive White Gaussian Noise (AWGN) and Land Mobile Satellite (LMS) channels, as well as real data tests. The results confirm the theoretical performance of the scheme for the selected messages. The last section in the paper presents the conclusions and the applicability of the proposed scheme to other cases.

2 | GENERAL CONSIDERATIONS

This section presents the message and channel assumptions and the performance metrics used.

2.1 | Message and channel assumptions

The proposed message M is divided into k pages (M_1, ..., M_k). We assume a multicast, many-to-many system, where several satellites transmit pages to many users. Each page has a parity check to tell if it is correctly received. Based on this parity check, we assume a page erasure channel. This means that the receiver knows whether each page is correctly received (parity check passed) or not (parity check failed). This assumption is realistic for GNSS messages: GPS L1 C/A messages include a 6-bit parity check for every 24 bits of data,[6] the Galileo Open Service (OS) E1 I/NAV includes a 24-bit Cyclic Redundancy Check (CRC) for every 2-second page of 250 bits in total,[1] and Galileo HAS E6-B C/NAV also includes a 24-bit CRC every 448-bit 1-second page.[7]

The message must be effectively encoded for different reception conditions, including urban canyons, foliage, or open-sky. Consequently, the analysis is based on both AWGN and fading (LMS) channels, and real data, with one or more satellites in view.

Notice that the focus of this work is not recovering parity-failed messages through error correction. The outer-coding scheme therefore does not focus on error correction capabilities by combining erased and not-erased pages. We assume that the likelihood of recovering information from an erased page is low. This is particularly true for Galileo I/NAV and C/NAV, where intrapage error correction already takes place through the Forward Error Correction (FEC) and interleaving,

implying that erased pages have generally a large quantity of errors. This assumption has been validated for the Galileo E6-B pages with real data.[8]

2.2 | User performance metrics

Standard coding references propose metrics such as coding gain, minimum distance, or coding rate[9] as coding design parameters. While some of these metrics will be qualitatively discussed in the article, the focus will be on the abovementioned TTRD. The schemes analyzed target the minimum theoretically achievable TTRD. This means that the coding scheme should minimize repetitions and that most or all correctly received pages contribute to the message. The article also analyzes the decoding complexity in the receiver.

Our problem can therefore be defined as follows: A message M consisting of k pages (M_1, ..., M_k) is encoded into a set C consisting of n pages (C_1, ..., C_n), such that when any subset C' of C k' pages (C'_1, ..., $C'_{k'}$) is received, the message can be decoded. In the coding theory nomenclature,[10] a coding scheme that achieves this property with $k' = k$ is considered as fully efficient, or a Maximum Distance Separable (MDS) code.

3 | OUTER CODE TRANSMISSION SCHEMES

This section describes outer code transmission schemes, including offsetting and coding schemes, and presents a qualitative comparison. By "outer code" it is meant that the message pages may be already encoded and therefore the proposed schemes focus on improving the reception of the full message, as opposed to the reception of each page by increasing the page coding gain. For example, Galileo E6-B pages are already protected by a convolutional code, which is considered the "inner code." The outer-coding schemes considered in this paper are illustrated in Figure 1, which depicts the message M of k pages transmitted by four satellites (SV1 to SV4) for a time interval of $2k$ time units, in which M is transmitted twice by each satellite. Figure 1 depicts the case of no encoding, no encoding with offset, Reed-Solomon codes[11] with offset, and Fountain codes[5] with offset. The pages at the start of the message are shown with a light shade, and the pages at the end of the message with a dark shade. The case of Fountain codes is also representative of the high-redundancy vertical Reed-Solomon codes explained later. The figure depicts one page per second being transmitted.

No Encoding

SV1	M_1	...					M_k	M_1	...			M_k
SV2	M_1	...					M_k	M_1	...			M_k
SV3	M_1	...					M_k	M_1	...			M_k
SV4	M_1	...					M_k	M_1	...			M_k

No Encoding + Offset

SV1	M_1	...					M_k	M_1	...			M_k
SV2	M_{j+1}	...			M_k	M_1	...	M_{j+1}	...		M_k	M_1	...
SV3	M_{2j+1}	...		M_k	M_1	...	...	...	M_{2j+1}	...	M_k	M_1	...	...	...
SV4		M_k	M_1	...			M_k	M_1	...	

RS + Offset

SV1	C_1	...					C_k	C_{k+1}	...	C_n	C_1	...	C_j
SV2	C_{k+1}	...	C_n	C_1		...	C_j	C_{j+1}	...			C_n
SV3	C_{j+1}	...					C_n	C_1	...			C_k
SV4	C_1	...					C_k	C_{k+1}	...	C_n	C_1	...	C_j

Fountain + Offset, High Redundancy RS + Offset

SV1	C_1	...			C_k	C_{k+1}	...	C_{2k}
SV2	C_{2k+1}	...			C_{3k}	C_{3k+1}	...	C_{4k}
SV3	C_{4k+1}	...			C_{5k}	C_{5k+1}	...	C_{6k}
SV4	C_{6k+1}	...			C_{7k}	C_{7k+1}	...	C_{8k}

FIGURE 1 Transmission of a long message by four satellites with No Encoding, No Encoding with offset, Single Reed-Solomon Code with offset, and Fountain Codes with offset/High-Redundancy Reed-Solomon vertical codes with offset

3.1 | No encoding

The same message is transmitted by all satellites without any encoding. When the message is finished, it is rebroadcast again. All satellites transmit the same page at a given time. The minimum TTRD is k seconds, and there is a high amount of repetitions, up to three per second if all four satellites are received. Also, if one page is lost, for example, due to the temporary occlusion of all satellites at the same time, another k seconds are required from the time the page is lost.

3.2 | No encoding with offset

The message is transmitted without encoding but with an offset between satellites (j in Figure 1). The scheme does not guarantee that there are no repetitions. The minimum TTRD in our example is k divided by the number of transmitters, assuming that each satellite transmits a sequence leading to no repetition, which is hardly achievable in GNSS due to geometrical reasons. A detailed performance analysis of this scheme is available in Fernández-Hernández et al.[12]

3.3 | Single Reed-Solomon code with offset

In this scheme, we assume that the message **M** is encoded with a Reed-Solomon code.[11] Reed-Solomon codes are a good candidate of block codes for erasure channels. They have the property sought in our problem statement: Any k symbols of the Reed-Solomon-encoded message **C** allow the full message retrieval. Reed-Solomon uses Galois Field GF(2^m) arithmetic, where m is the symbol size and defines the field size, 2^m, allowing the transmission of a message of a maximum of $N = 2^m - 1$ symbols. Typically, Reed-Solomon codes use $m = 8$ bits. This allows a maximum of $N = 255$ eight-bit encoded pages for a total of 2040 bits including parity. This means that the original message must be shorter than this length, which seems insufficient for long GNSS messages. For a long message with a high redundancy, higher values of m can be sought, eg, $m = 16$, allowing up to $N = 2^{16} - 1$. However, these are much more computationally expensive and less standardized. In particular, the decoding cost grows exponentially with n, as the number of decoding operations can be estimated as $k(n - k)\log_2 n$. This makes the parallel Reed-Solomon codes described later superior from the computational

cost point of view. Figure 1 depicts an implementation of a single Reed-Solomon code encoding the message and including some offsetting between satellites. Due to the restrictions in the amount of parity $(n - k)$ pages for $m = 8$, the message will not be long enough to avoid repetitions, especially in case of multiple satellites. Reed-Solomon coding in this fashion has already been proposed in GNSS for the QZSS CLAS service[2] and for Galileo I/NAV message improvements.[13]

3.4 | Fountain codes

Fountain codes, or *rateless* codes,[5] are also suitable for channels with erasures. They allow the retrieval of the message with k' pages, with k' equal to or slightly higher than k. For example, for binary random linear fountain codes, the expected value of k', $E(k')$, is bounded by the function $2^{-\delta}$, where δ is the excess number of pages. Therefore, if the expected overhead $(k' - k)$ is small, they are good candidates for an outer code for long messages in typical GNSS reception conditions. There are several implementations possible, including random linear codes, Luby Transform (LT) codes,[14] or Raptor codes.[15] Fountain codes may require the receiver and the transmitter to share an encoding/decoding matrix. The size of this matrix is limited by the maximum reception time expected, which should lead to an affordable size for a GNSS receiver. However, the encoding/decoding process can also be performed on the fly. In this case, the system may allocate bandwidth to transmit the decoding matrix or preferably use methods allowing the receiver to generate the matrix according to a pseudorandom process based on the packet number.

Fountain codes have already been studied for GNSS.[3,16] They show good results for short pages (eg, 8 bits) and messages of some hundreds of pages long, both in terms of reception and decoding computational cost. However, Fountain codes always have an expected overhead, ie, $E(k') > k$. If packets are long with respect to the total message length, even a one-packet overhead can be significant. For example, in the case of Galileo HAS, a message can be as short as two packets (or 448-bit pages), and thus a one-packet overhead may be very significant. Also, the most efficient implementations of Fountain codes, such as Raptor codes, are subject to patents.

Figure 1 shows that, since Fountain codes are rateless, they can be transmitted for an n as high as necessary, and determined dynamically. The figure also shows that, as there are no limits for the message parity, different satellites can transmit different parts of the message by offsetting the message pages, as described in Fernández-Hernández et al.[3] As the selected scheme can

be encoded in a similar way as Fountain codes (with the difference that $k = E(k')$), it is also depicted in Figure 1 together with Fountain codes.

Another scheme recently proposed in the GNSS literature is based on Low-Density Parity Check (LDPC) codes combined with a low-rate message repetition. It is described and characterized in Tarable et al.[16] Similar to Fountain codes, this scheme is capable of reconstructing the message with a near-ideal performance regarding the MDS property (ie, with k' slightly higher than k).

4 | HIGH-PARITY VERTICAL REED-SOLOMON CODING

As mentioned above, the main limitation of standard Reed-Solomon implementations is that the Galois Field cannot accommodate a long message with a very high parity that allows no repetitions with multiple transmitters. In order to overcome this problem, instead of encoding "horizontally" all the symbols of the message into one Reed-Solomon code, the proposed scheme *encodes vertically every column* of symbols of every page for a total of J Reed-Solomon codes. The concept is illustrated in Figure 2. Then, different subsets of the encoded pages $C_{i = 1...n}$ are transmitted by different satellites. When the receiver collects k pages, it decodes the J codes with the same decoding matrix and obtains the original message. This allows one to multiply by J the length of the encoded message at no performance degradation
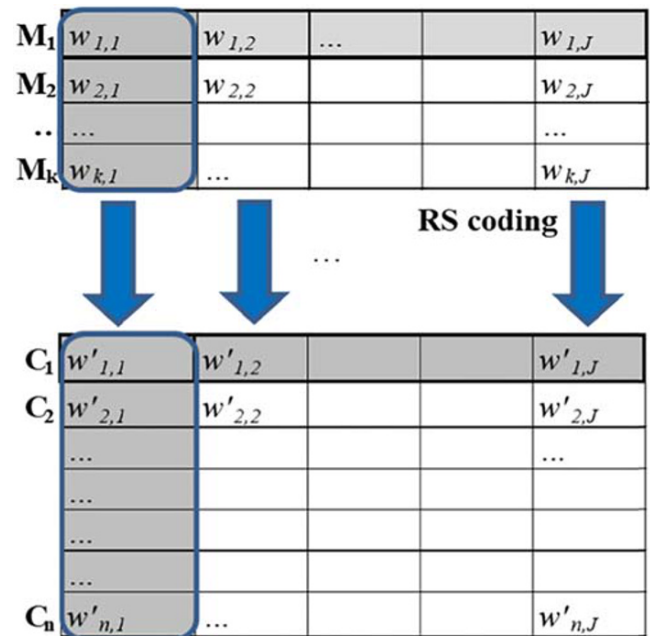

FIGURE 2 Outer code—encoding process [Color figure can be viewed at wileyonlinelibrary.com and www.ion.org]

without significantly increasing the decoding complexity at the receiver side and preserving the *no repetition* property even with many transmitters. While such vertical encoding schemes have been proposed for data backup systems,[17] they have never been adopted before for radio navigation, to the knowledge of the authors.

4.1 | Message encoding and transmission

The proposed outer-coding scheme is illustrated in Figure 2 and is based on the following steps:

- A standard Reed-Solomon code RS(N, K, m) is selected as a reference, where m is the symbol size, N is $2^m - 1$, and K is the maximum number of information symbols. As for any Reed-Solomon code, a primitive polynomial $g(x)$ of order m, defining the multiplication operation within the Galois Field, is selected.
- The message $\mathbf{M}$ is divided into k pages of J symbols each. The message content of each page is divided into symbols: $w_{1,1}$ to $w_{1,J}$ for the first page M_1, and so on. In this case, $m = 8$, and the symbols correspond to octets.
- The symbols are vertically grouped into J information words of length k, from $w_{1,1}$, $w_{2,1}...w_{k,1}$ for the first symbol of all pages to $w_{1,J}$, $w_{2,J}...w_{k,J}$ for the last one. If $k < K$, the remaining $K - k$ octets are *shortened*, ie, filled with zeroes, as shown at the top of Figure 3 where the region in zeroes is colored in black.
- Each vertical information word is encoded with the RS(N, K, m) code. Reed-Solomon encoding is defined in detail in Wicker and Bhargava[4] and Westall and Martin[18] and is summarized in the following steps for each $j = 1...J$:

○ Generation of the Vandermonde matrix $\mathbf{V}_{(N,K)}$ of N rows and K columns, defined as

$$\mathbf{V} = \begin{bmatrix} 0^0 & \cdots & 0^{(K-1)} \\ \vdots & \ddots & \vdots \\ (2^N-1)^0 & \cdots & (2^N-1)^{K-1} \end{bmatrix}. \tag{1}$$

○ Generation of the encoding matrix $\mathbf{D}_{(N,K)}$ from $\mathbf{V}$ through linear transformations, eg, through the Gaussian elimination method, where $\mathbf{D}$ is defined as

$$\mathbf{D} = \begin{bmatrix} \mathbf{I} \\ \mathbf{P} \end{bmatrix}, \tag{2}$$

and where $\mathbf{I}$ is the (K, K) identity matrix that makes the code systematic and $\mathbf{P}(N - K, K)$ is the remaining part providing the parity.

○ Encoding of the message $\mathbf{M}^{(j)}$ into $\mathbf{C}^{(j)}$, the vertically encoded message.

$$\mathbf{D} \cdot \mathbf{M}^{(j)} = \mathbf{C}^{(j)}. \tag{3}$$

- The vertically encoded symbols are referred to as $w'_{i,j}$ in Figure 2, where $i = 1...n$ and $j = 1...J$. Note that, as
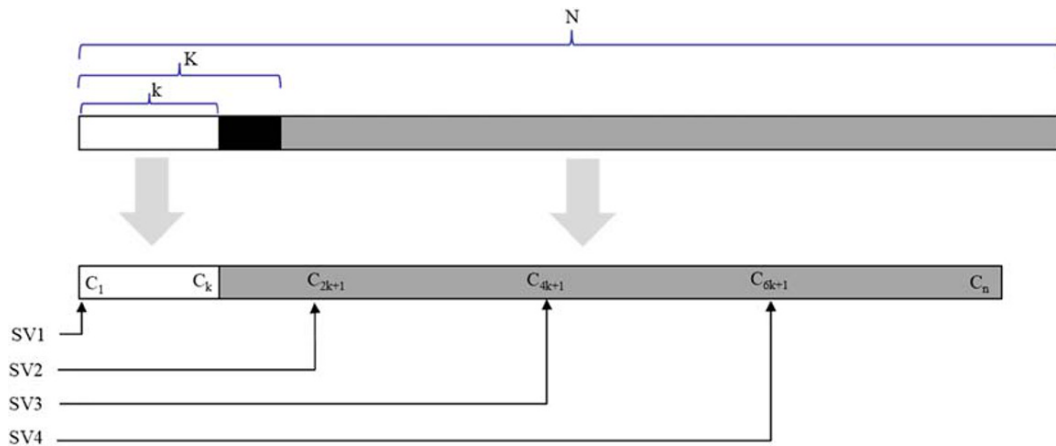

FIGURE 3 High-parity Reed-Solomon encoding of each vertical code of k symbols into $n = N - K + k$ symbols, and transmission of the encoded message by four satellites (SV1 to SV4), with an offset of $2k$ packets between satellites, guaranteeing no repetition for a transmission period of two full messages ($2k$) [Color figure can be viewed at wileyonlinelibrary.com and www.ion.org]

Reed-Solomon codes are systematic codes, $w_{1,1}...w_{k,J} = w'_{1,1}...w'_{k,J}$.

- The symbols are grouped horizontally into pages as per Figure 2, where the first encoded page $\mathbf{C}_1$ is composed by $w'_{1,1}...w'_{1,J}$, etc, up to the n pages $\mathbf{C}_1...\mathbf{C}_n$.

The encoded message is transmitted as follows:

- Each encoded page is encapsulated with a page header that includes the message ID, the page ID $(1...n)$, and the original message size k. This information is necessary for the receiver, as this allows the transmitting system to perform *puncturing* and dynamically allocate encoded pages to transmitters. The $K - k$ pages $\mathbf{C}_{k+1}...\mathbf{C}_K$ are not allocated for transmission as they include only zeroes.
- Each satellite is allocated an offset in order to guarantee the no repetition property during the transmission period. As an example, Figure 3 at the bottom shows an offset of $2k$ for four satellites, SV1 to SV4, where, for the first $2k$ seconds, SV1 transmits packets $\mathbf{C}_1$ to $\mathbf{C}_{2k}$, SV2 transmits packets $\mathbf{C}_{2k+1}$ to $\mathbf{C}_{4k}$, and so on.

4.2 | Message reception and decoding

Figure 4 describes the decoding process. It is based on the following steps:

- The receiver assembles the encoded message $\mathbf{C}'$ composed of the k pages correctly received.
- The k rows of $\mathbf{D}$ corresponding to the $\mathbf{C}'_1...\mathbf{C}'_k$ received pages are used to generate the encoding sub-matrix $\mathbf{D}'$, which is inverted into $\mathbf{D}'^{-1}$.
- Each of the $j = 1...J$ vertically encoded messages is decoded separately by multiplying it with $\mathbf{D}'^{-1}$. For each vertical message $\mathbf{M}^{(j)}$,

$$\mathbf{M}^{(j)} = \mathbf{D}'^{-1} \cdot \mathbf{C}'^{(j)}, \qquad (4)$$

where $\mathbf{C}'^{(j)}$ is the received vertically encoded word in column j, until the original message $\mathbf{M}$ is retrieved.

5 | PARTICULARIZATION FOR HIGH ACCURACY

This section particularizes the proposed scheme for the Galileo HAS. The purpose of the Galileo HAS is to allow users to calculate a high-accuracy position as fast as possible through Precise Point Positioning (PPP) techniques. In order to do that, the receiver needs to obtain accurate satellite orbit and clock corrections, interfrequency biases, and possibly ionospheric corrections from the Signal In Space (SIS).

5.1 | Galileo HAS message

The Galileo HAS message will be transmitted in the C/NAV pages of the E6-B Galileo signal component at a carrier frequency of 1278.75 MHz[1, 19] (see also Table 1). The C/NAV page layout is shown in Figure 5. 492 bits are encoded into 984 symbols and then interleaved.[19] The transmission of a page starts with the transmission of the first bit of a 16-bit synchronization pattern, which coincides with the start of an integer Galileo System Time (GST) second. Out of 492 bits available, 14 bits are reserved for other services, 448 bits are used for the HAS page, 24 bits are used by the CRC, and 6 bits are used for the tail of the convolutional code used to protect the transmitted symbols. We focus on the 448 bits of the HAS page and use the CRC result as a basis for our erasure channel assumption. Within the HAS page, 24 bits are devoted for the header, including message ID (up to 4 bits), page ID (up to 8 bits), and message length k (up to 5 bits), plus other fields, and 424 bits are devoted to the
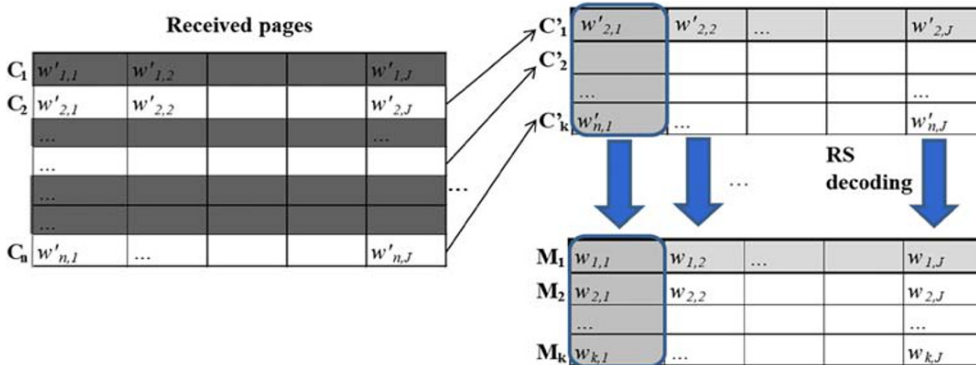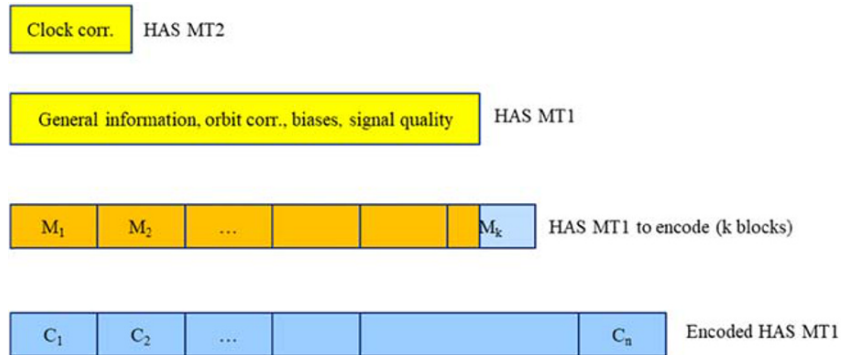

FIGURE 4 Outer code—decoding process. Erased pages are depicted in dark gray in the left figure. The remaining k pages are grouped into the encoded C' message, which is vertically decoded j times to form the original message M [Color figure can be viewed at wileyonlinelibrary.com and www.ion.org]

TABLE 1 C/NAV page

Sync	Information Symbols			Total
16	984			1000
C/NAV Page (information bits)				
Reserved	HAS Page	CRC	Tail	Total
14	448	24	6	492
HAS Page (information bits)				
HAS Page Header	HAS Message			Total
24	424			448

time [s]	0	1	2	3	4	5	6	7	8	9	10
										MT2	
				MT1							

FIGURE 6 MT1 (light gray) and MT2 (dark gray) distribution

- One GPS code bias and carrier phase bias;
- Three Galileo code and carrier phase biases;

This leads to a 15-page MT1 of 6360 bits and a 2-page MT2 of 848 bits. The MT1/MT2 sequence allocation is depicted in Figure 6. Every 10 seconds, eight MT1 pages and two MT2 pages are transmitted synchronously by each

FIGURE 5 HAS message structure, including MT2 (clocks) and MT1 (orbits and other information), with MT1 before and after coding [Color figure can be viewed at wileyonlinelibrary.com and www.ion.org]

page content. Two HAS messages are defined for this work: a first Message Type, called MT1 in this paper, which carries the general HAS information, satellite and signal masks, orbital corrections, biases, and signal quality monitoring, and a second one, called MT2, which contains the clock corrections and may require a higher update rate. MT2 is a short message and is less demanding for the proposed outer code. Before a message is encoded, if its length does not coincide with a multiple of 424 bits, it will be filled in with a chain of zeroes and ones of the required length.

The proposed format is flexible in size for each MT, depending on the number of satellites in the mask and signals corrected. In order to maximize compatibility and interoperability, the message structure is based on the Radio Technical Commission for Maritime (RTCM) Standard, and in particular the Compact State-Space Representation (CSSR) format,[20] as is the case for QZSS CLAS service. The detailed content and format of HAS falls beyond the scope of this article.

For the reported tests, we defined MT1 and MT2 with these assumptions:

- Orbit and clock corrections transmitted for 28 GPS and 26 Galileo satellites;

satellite. We have also assumed that MT2 is updated every 10 seconds and MT1 is updated every 120 seconds.

5.2 | Galileo HAS message encoding and satellite allocation

Each vertical information word is encoded through a Reed-Solomon code RS(255, 32, 8) with the following primitive polynomial $g(x)$:

$$g(x) = x^8 + x^4 + x^3 + x^2 + 1. \tag{5}$$

The polynomial corresponds to that already used for the optimized transmission of Galileo clock and ephemeris data proposed for I/NAV.[13] The 424-bit HAS page is divided into 53 eight-bit symbols ($J = 53$) and vertically encoded as described above. With this configuration, a message of up to 32 [symbols] · 8 [bits] · 53 [vertical codes] = 13 568 bits can be encoded. This seems sufficient for all types of HAS messages envisaged at the moment. In the proposed 15-page MT1, $k = 15$ and $n = N - K + k = 255 - 32 + 15 = 238$. This allows a minimal coding rate of $r = n/k = 0.063$. This extremely low coding rate does not penalize the transmission
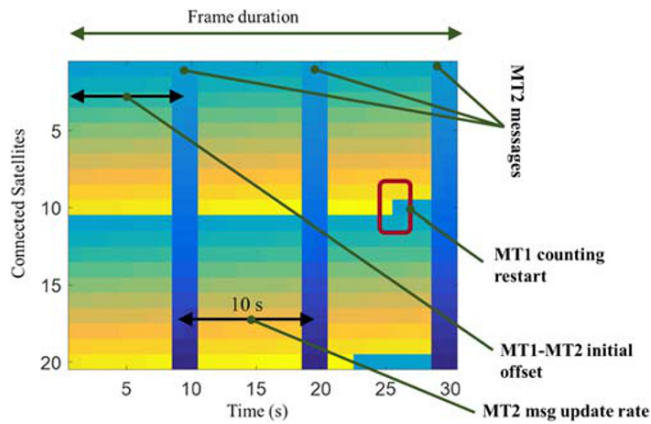
FIGURE 7 MT1 and MT2 distribution over a 30-second frame, and allocated to 20 transmitting (connected) satellites, over a 30-second HAS frame [Color figure can be viewed at wileyonlinelibrary.com and www.ion.org]

performance of HAS, as a given MT1 will be transmitted anyway for around 1 minute, as is the case of, for example, the satellite ephemerides for much longer time intervals, on the order of hours. On the contrary, this very low coding rate (or very high parity) allows allocating different pages to different satellites and, with an adequate satellite allocation algorithm, ensures no repetition in any receiver on Earth. Figure 7 depicts an allocation strategy where the encoded pages $C_1...C_{238}$ are allocated to 10 different satellites. As the Galileo-transmitting satellites are reduced to 20 (out of the total minimum of 24 satellites) in the first generation full-operational capability configuration, the system can ensure by assigning the same sequences to satellites at the other side of the orbit that there are no repetitions or their probability is almost negligible. This assumption is further developed in Appendix A.

Notice that the outer code allows puncturing, so not all of these pages are needed to be transmitted by a satellite. This is particularly true for the case of MT2, which is shorter and does not require the use of the full parity.

6 | PERFORMANCE RESULTS

This section analyzes the TTRD obtained by high-parity vertical Reed-Solomon codes for the high-accuracy message described in the previous section. It also analyzes the decoding complexity. First, simulated results are presented using AWGN, LMS, and a rural pedestrian model with one and two transmitting satellites. This is followed by real data results with two and four satellites.

6.1 | Simulated data analysis

In this section, TTRD is analyzed with a MATLAB simulator tool. The tool emulates everything that concerns the message generation, transmission, and decoding. Except when noted, the receiver is assumed in ideal tracking conditions. The tool has the capability to configure AWGN and LMS channels with a dynamic time series of attenuation. It is also possible to configure an external channel time series from real measurements. The receiver model gets the symbols out of the channel and performs the decoding into information bits, checking at the end if the information decoded is equal to that transmitted. TTRD is calculated as the time to get both MT1 (15 pages) and MT2 (2 pages), as described in the previous section.

Table 2 shows the results of the simulations for 1-hour tests in an AWGN channel with C/N_0 of 45 and 29 dBHz. At 45 dBHz, no bit errors are observed, and thus the TTRD is simply related to the reception time of the pages, taking advantage of the redundancy provided by the two satellites. At 29 dBHz, the number of bit errors becomes relevant, but nevertheless, the TTRD stays on the order of 20 to 30 seconds for most of the time.

Table 2 also presents the results in an LMS channel environment. The channel model used is the narrow-band two-state as described by Prieto-Cerdeira et al.[21] The model assumptions are described in Table 3. Two uncorrelated 1-hour time series for simulating two

TABLE 2 TTRD values—Simulated results of the vertical Reed-Solomon proposed scheme (VRS) for AWGN, LMS, and Rural Pedestrian, and comparison with the cases of No Encoding (NE), No Encoding with Offset (NEO), and Single Reed-Solomon with Offset (SRSO) for AWGN-29dBHz and LMS

	N° Sats	TTRD, s		
		Avg	95%	Max
VRS-AWGN—45 dBHz	2	12.2	14	14
VRS-AWGN—29 dBHz	2	21.7	30.0	52.0
VRS-LMS	2	24.8	39.0	58.0
NE-AWGN—29 dBHz	2	52.0	83.0	115.0
NEO-AWGN—29 dBHz	2	49.0	81.0	106.0
SRSO-AWGN—29 dBHz	2	30.0	42.0	68.0
NE-LMS	2	41.0	78.0	104.0
NEO-LMS	2	45.0	90.0	109.0
SRSO-LMS	2	39.0	61.0	80.0
VRS-Rural Ped. 20°	2	12.7	17.0	40.0
VRS-Rural Ped. 20°	1	24.9	34.0	77.0

TABLE 3   Assumptions for LMS channel model

Channel Model	2-State
Environment	Urban
Satellite elevation, deg	40°
User speed, km/h	50
LOS C/N_0, dBHz	35
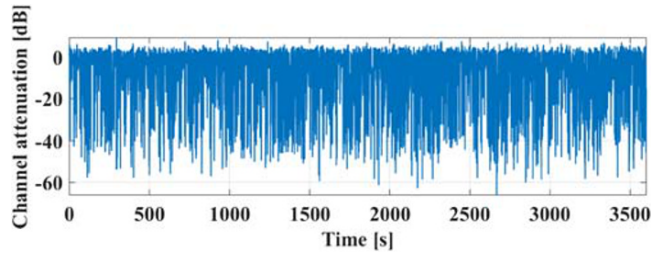
FIGURE 8   Channel time series showing signal attenuation [dB] for one satellite as per LMS model [Color figure can be viewed at wileyonlinelibrary.com and www.ion.org]

satellites at an elevation of 40° were generated using this channel model.

The LMS channel imposes a considerable stress on the transmission scheme due to the frequent drops in signal power as we can observe in Figure 8. In this scenario, the TTRD does not exceed an average of 25 seconds with a 95%-quantile value of 39 seconds.

The last rows of Table 2 present the comparison of the proposed vertical Reed-Solomon scheme with the transmission strategies *No encoding*, *No encoding with offset*, and *Single Reed-Solomon code with offset* defined in the previous section. The *No encoding with offset* scheme is implemented with a between-satellite offset of eight pages for MT1 and one page for MT2, which is the best-possible offset in this scenario. The *Single Reed-Solomon code with offset* scheme cannot be directly implemented for MT1, due to its length, so MT1 is divided in five separately encoded blocks and transmitted with a between-satellite offset of 8 seconds. The 29-dBHz scenario shows TTRDs between 42 and 83 seconds (95%), and the LMS scenario between 61 and 90 seconds (95%), all significantly higher than the TTRDs obtained with the proposed scheme.

Finally, a rural pedestrian channel model derived from real measurements obtained by the GSA (European GNSS Agency) was used, assuming one or two satellites at an elevation of 20° with an aggregated probability of successful decoding of 0.79, including the Page Error Rate (PER) and tracking availability. Even in the extreme case of one transmitting satellite, the TTRDs are 24.9 seconds in average and 34 seconds as 95% quantile, while

the same values considering two satellites are 12.7 and 17 seconds, respectively.

In addition to the TTRD characterization, a preliminary analysis of the decoding cost of a HAS 15-page MT1 has been performed. The decoding operations analyzed include one [K, K] matrix inversion ($\mathbf{D}'$ into $\mathbf{D}'^{-1}$) and j matrix multiplications of Equation (4), where $K = 32$ and $J = 53$. Other methods are possible given that the decoding process only requires solving a linear system of k equations with k unknowns, where $k = 15$. The analysis was done with MATLAB_R2016b including 900 decoding trials. The laptop used has a 2.7-GHz i5 7200U CPU with 8 GB of RAM. The average decoding time was 0.12 seconds, mostly devoted to the matrix inversion. This shows that the decoding cost even with a non-optimized MATLAB implementation is affordable. Future analyses will characterize the computational burden of real implementations in different types of receivers.

6.2 | Real data analysis

Several data collections involving the reception of E6-B signals were performed and used to characterize the performance of the proposed Reed-Solomon coding scheme. While the complete empirical analysis of the proposed Reed-Solomon encoding scheme is out of the scope of this paper, preliminary results considering a dynamic scenario are presented.

At the time of the test, Galileo E6-B satellites broadcast dummy messages that are known at the receiver side. Thus, it was possible to evaluate channel effects and determine when bit errors occur.[8] In the experiments performed, bit error time series were extracted from the received Galileo E6-B signals and used to model the reception channel. The dissemination scheme described above with 15 MT1 pages and two MT2 pages and depicted in Figure 7 was adopted and generated. Page reception was determined according to the error patterns extracted from real data.

The experiments were conducted using a van equipped with a Trimble Zephir antenna capable of receiving Galileo E6 signals. Data were collected using a Septentrio AsteRx4 receiver. Views of the experimental setup adopted for the test are provided in Figure 9. Figure 9b shows the Septentrio receiver installed inside the van along with additional equipment used for other experiments.

Two tests were performed inside the Joint Research Centre (JRC) in Ispra, Italy. During such tests, the van performed several laps according to the trajectories shown in Figure 10. The striped curve in Figure 10 corresponds to the first experiment denoted here as Test A,
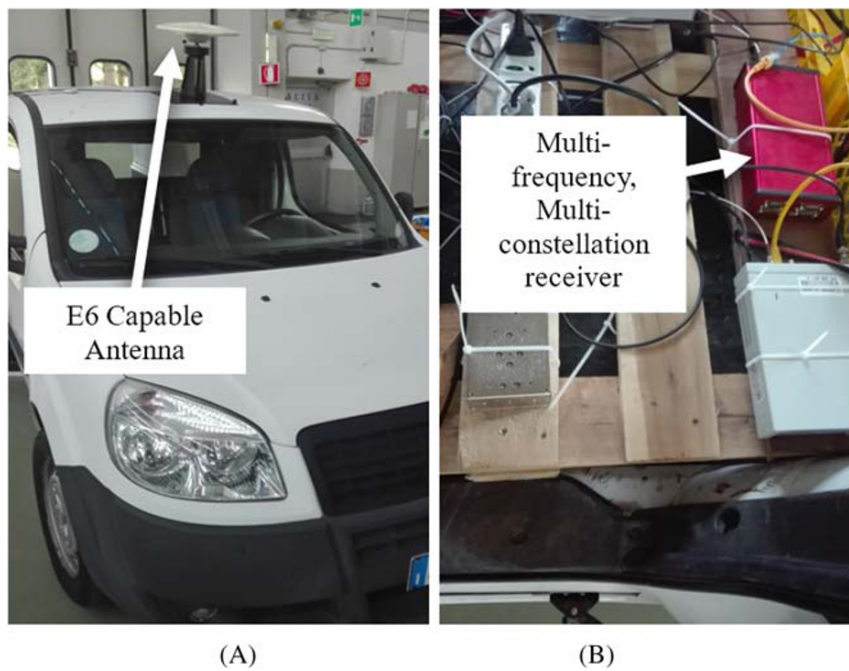
FIGURE 9 Experimental setup adopted for the collection of Galileo E6-B signals. (a) Exterior of the van equipped with a Galileo E6 capable antenna and (b) interior of the van with the multifrequency, multiconstellation receiver used for the data collection [Color figure can be viewed at wileyonlinelibrary.com and www.ion.org]


FIGURE 10 Trajectories performed during the two dynamic experiments. The striped curve corresponds to Test A whereas the continuous line is relative to Test B [Color figure can be viewed at wileyonlinelibrary.com and www.ion.org]

whereas the continuous line is relative to the second test and it is labeled as Test B. During the two tests, four Galileo E6-B signals were tracked. The JRC campus is characterized by tall trees and buildings causing signal erasures.

For this reason, the C/N_0 estimated from the received signals is affected by severe oscillations.

Signal reception conditions are analyzed in Figure 11, which provides the estimated C/N_0 for the four signals

FIGURE 11 Signal reception conditions observed during the E6-B dynamic experiment. (a) C/N$_0$ recorded for the four E6-B signals tracked as a function time. (b) Erasures occurring during the reception of the E6-B pages [Color figure can be viewed at wileyonlinelibrary.com and www.ion.org]
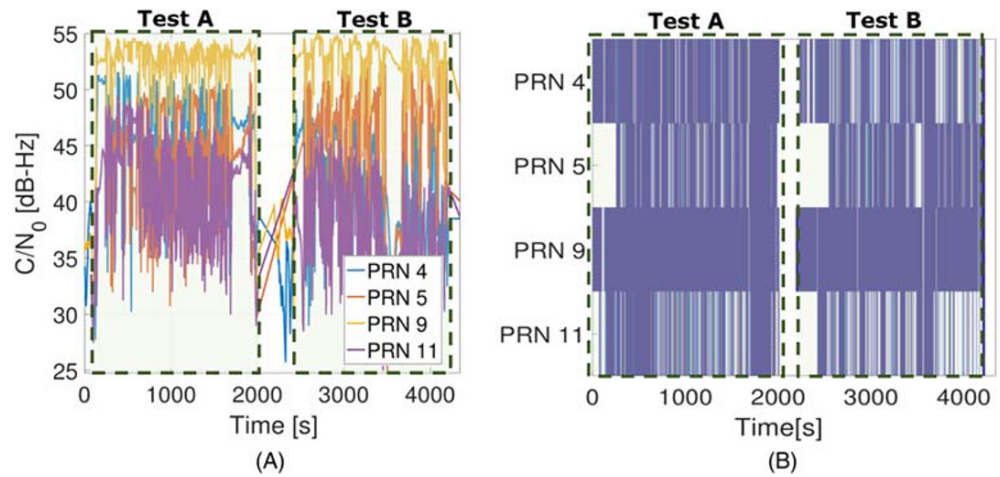
tracked (left part) and indicates the occurrence of erasures in the E6-B navigation message (right part). Figure 11a shows oscillations in the estimated C/N$_0$ due to the motion of the vehicle through the different obstacles and obstructions present in the JRC campus. The signal from satellite PRN 9 is characterized by a high elevation and a strong C/N$_0$. In this case, pages are correctly extracted most of the time with a page availability close to 84%. The signal from satellite PRN 11 is the weakest and page availability is reduced to 46%. Figure 11b shows the occurrence of page erasures. White areas in the figure indicate that the page was lost and the receiver was unable to track the signal. Dark areas indicate that E6-B pages were correctly decoded, whereas light tones in the figure indicate that a page was received with errors. Our analysis considered this last type of pages as erased pages. From the figure, it emerges that only a few pages are received with errors. This result confirms the validity of the erasure assumption where most of the pages are either correctly received or are not decoded.

Using these configurations, it was possible to evaluate the TTRD under real reception conditions. The results are summarized in Table 4, which provides the TTRD statistics. The TTRD has been computed considering two cases:

1. all four available satellites are used for message retrieval.
2. only two satellites are used for message retrieval. In this second case, the two satellites are randomly selected out of the four for each TTRD calculation, and the statistics provided in Table 4 were obtained by averaging the results with respect to the satellite pair extraction.

The availability of four satellites significantly reduces the average TTRD, which is lower than 8 seconds for both Test A and Test B. Under such conditions, the maximum TTRD is significantly lower than 30 seconds for both test cases.

When the number of satellites is reduced to two, statistics close to those of the simulated rural scenario are obtained. In particular, the average TTRDs are close to the values reported in Table 2. It is noted that for Test B, a quite large maximum TTRD (84 seconds) is observed. This case corresponds to the situation where signals PRN 5 and PRN 11 are selected. In particular, it clearly emerges from Figure 11b that the receiver had difficulties acquiring and tracking these two signals at the beginning of Test B. Under such conditions, no E6-B pages are extracted and long TTRDs are observed.

Despite this fact, the experimental results are in accordance with the simulation findings presented above and further support the effectiveness of the proposed encoding scheme.

7 | CONCLUSION AND WAY FORWARD

At the current power levels and bit rates, the timely and robust transmission of GNSS messages of several thousand bits for uses such as PPP, authentication, or long-

TABLE 4 TTRD evaluated considering real E6-B data under dynamic conditions

	TTRD, s		
	Avg	95%	Max
Test A, four satellites	7.47	9.0	16.0
Test B, four satellites	7.96	11.0	20.0
Test A, two satellites	13.58	22	44
Test B, two satellites	15.69	32	84

term ephemerides, remains a challenge. The assumption that the long message is divided into pages, each with a parity check, and transmitted through an erasure channel, seems a plausible one for the particular case of Galileo I/NAV and C/NAV message structure, but also more generally for GNSS and potentially other systems. Based on this assumption, an outer-coding scheme is sought for long message transmission. This scheme should be computationally easy to decode and allow that all well-received pages contribute to the message with no repetitions.

After a review of message partitioning and encoding schemes in the literature, this paper proposes a scheme that achieves these properties. The scheme is based on vertically encoding each symbol of a page in a separate Reed-Solomon code based on a Galois Field of 256 8-bit elements with very high parity. It then allocates different parts of the encoded message to different satellites, ensuring no repetitions for all users worldwide for intervals well beyond the expected reception time. To the knowledge of the authors, such a scheme has not been proposed for radio navigation, yet it highly simplifies the implementation of block codes such as Reed-Solomon codes.

The scheme is particularized for Galileo HAS messages of 6360 bits, including orbits, biases, and general HAS information, and 848 bits, including clock information, for a total of 54 Galileo and GPS satellites. The messages are partitioned in 448-bit E6-B pages according to the current Galileo C/NAV message definition. The TTRD of this scheme is measured in simulated scenarios (AWGN, LMS, rural pedestrian) and real scenarios, with configurations between one and four transmitting satellites in view including severely degraded conditions. The results confirm the no-repetition property for the current implementation case. The two HAS messages can be received in a period between 9 seconds (95th percentile) with four transmitting satellites in view but with continuous fading in a real dynamic scenario, to below 40 seconds (95th percentile) in the worst-case scenarios, including LMS urban situations, and scenarios with only one satellite visible. The decoding complexity is expected to be very low. This is preliminarily tested with a MATLAB implementation and will be further analyzed with real implementations.

The proposed scheme is not only adequate for Galileo HAS but can also be used for any other long messages that are partitioned in pages and transmitted by one or several transmitters under noisy channels, including GNSS or other applications.

ORCID

Ignacio Fernández-Hernández https://orcid.org/0000-0001-9207-0775
Daniele Borio https://orcid.org/0000-0003-3573-5093

REFERENCES

1. European Union. *OSSISICD: Open Service Signal In Space Interface Control Document*. Issue Issue 1.3; 2016.
2. Cabinet Office. *Quasi-Zenith Satellite System Interface Specification Centimeter-Level Augmentation Service (IS-QZSS-L6–001)*. Draft Edition, 2017.
3. Fernández-Hernández I, Calle D, Cancela S, et al. Fountain codes for GNSS. In *Proceedings of the 30th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2017)*. Portland, OR; September 2017: 1496–1507.
4. Wicker SB, Bhargava VK (Eds). *Reed-Solomon Codes and Their Applications*. New York: John Wiley & Sons; 1999.
5. MacKay D. Fountain codes. *IEE Proc-Commun - Cap Approach Codes Des Implement Special Sect*. 2005;152(6):1062-1068.
6. US Government, GPS Directorate. NAVSTAR GPS Space Segment/Navigation User Segment Interfaces - IS-GPS-200-K. 2019.
7. Göhler E, Krol I, Bodenbach M, Winkel J, Seco-Granados G, Fernandez-Hernandez I. A Galileo E6-B/C receiver: signals, prototype, tests and performance. In *Proceedings of the 29th International Technical Meeting of the Satellite Division of the Institute of Navigation (GNSS + 2016)*. Portland, OR; September 2016:486–496.
8. Borio D, Susi M, Senni T, Fernández-Hernández I. The Galileo E6-B propagation channel: an experimental characterization. In *Proceedins of the 25th Ka and Broadband Communications Conference*. Sorrento, Italy; 2019.
9. Goldsmith A. *Wireless Communications*. Cambridge, UK: Cambridge University Press; 2005.
10. Singleton R. Maximum distance q-nary codes. *IEEE Trans Inform Theory*. 1964;10(2):116-118.
11. Reed IS, Solomon G. Polynomial codes over certain finite fields. *J Soc Ind Appl Math*. 1960;8(2):300-304.
12. Fernández-Hernández I, Calle JD, Cancela S, Pozzobon O, Sarto C, Simón J. Packet transmission through navigation satellites: a preliminary analysis using Monte Carlo simulations. In *ENC 2017*. Lausanne, Switzerland; May 2017: 298–304.
13. Schotsch BE, Anghileri M, Burger T, Ouedraogo M. 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)*. Portland, OR; September 2017: 1544–1558.

14. Luby M. LT Codes. *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*. 2002: 271–280.

15. Shokrollahi A. Raptor codes. *IEEE/ACM Trans Netw (TON)*. 2006;14(SI):2551-2567.

16. Tarable A, Andreotti R, Luise M, Zanier F, Cioni S. Link-layer coding for GNSS navigation messages. *NAVIGATION*. 2018;65: 405-421.

17. Planck JS. A tutorial on Reed-Solomon coding for fault-tolerance in RAID-like systems. 1996.

18. Westall J, Martin J. *An introduction to Galois Fields and Reed-Solomon coding*. Clemson, SC: School of Computing, Clemson University; 2010.

19. European Union. E6-B/C Signal-In-Space Technical Note. 2019.

20. Hirokawa R, Sato Y, Fujita S, Miya M. Compact SSR messages with integrity information for satellite based PPP-RTK service. In *Proceedings of the 29th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2016)*. Portland, OR, September 2016:3372–3376.

21. Prieto-Cerdeira R, Perez-Fontan RF, Burzigotti P, Bolea-Alamañac A, Sanchez-Lago I. Versatile two-state land mobile satellite channel model with first application to DVB-SH analysis. *Int J Satell Commun Netw*. 2010;28(5–6): 291-315.

APPENDIX A: | GEOMETRICAL CONSIDERATIONS ON PAGE-TO-SATELLITE ALLOCATION

This appendix presents the geometrical constraints in assigning the same code sequence to two satellites of a GNSS constellation while ensuring no page repetition for any user on Earth. In order to do this, a system can assign the same sequence to antipodal satellites in a given orbital plane. However, a satellite may not be always found exactly in the opposite angle of the orbit and therefore some tolerance may be required. This tolerance is analyzed here. This appendix presents how to calculate the surface at which the antipodal satellite can be found and still ensure that no user on Earth can see the two satellites at or above a given elevation.

As shown in Figure 12, one can determine α, which is the solid angle in the orbital sphere, or the arc in the orbit, from the transmitting satellite, where the antipodal satellite can be placed. α can be calculated as a function of the elevation e by solving nonlinear Equation (A3), which isolates h from Equations (A1) and (A2), where A is the Galileo orbital radius (29 599.8 km) and R is the Earth radius (6371 km). Then, as shown in Equation (A4), we can calculate θ, which defines the same arc but from the Earth center. The arc of the orbit where the satellite with the same sequence can be placed, is 2θ.
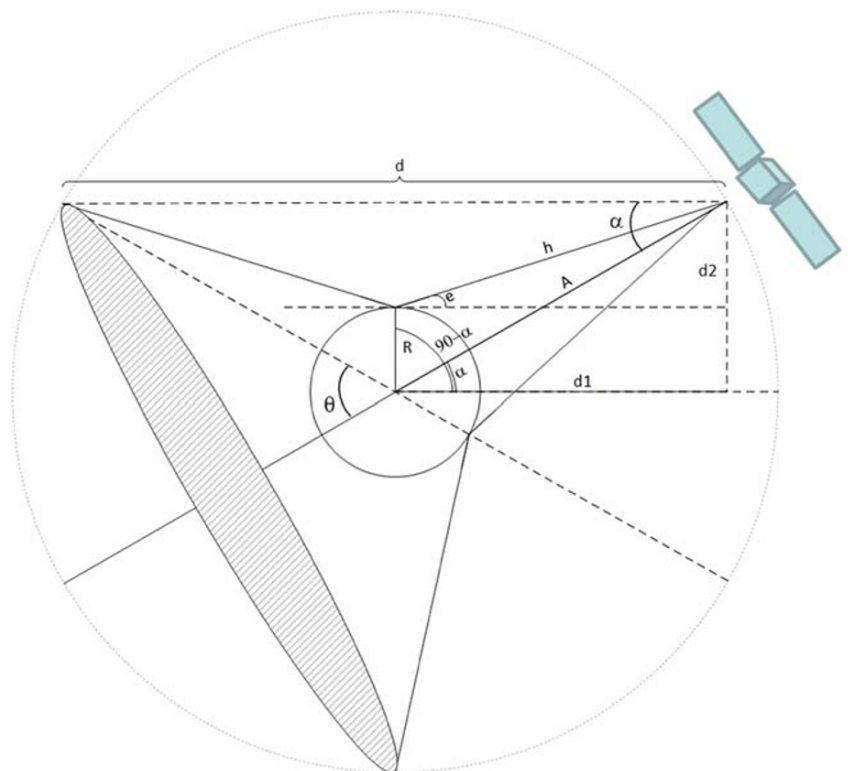

FIGURE 12 Satellite distance d between two satellites that ensures no repetition for any user with a masking angle of *e* [Color figure can be viewed at wileyonlinelibrary.com and www.ion.org]
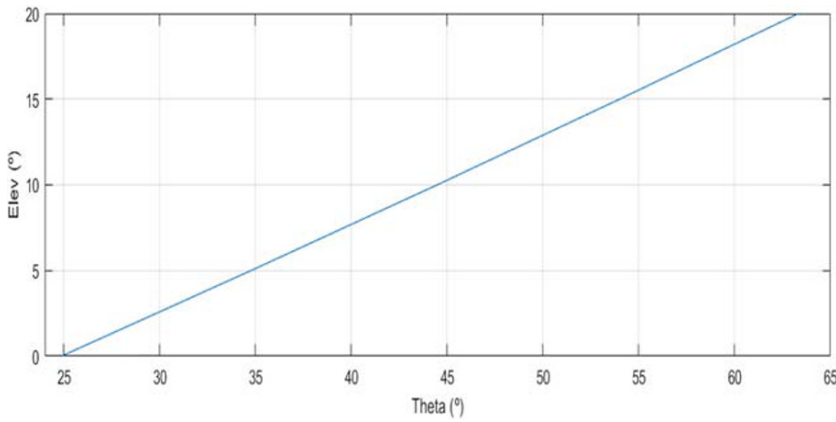
FIGURE 13 Relationship between θ and e, where 2θ is the arc within the satellite orbit where the antipodal satellite can be located and not seen by any user on Earth with a masking elevation of e [Color figure can be viewed at wileyonlinelibrary.com and www.ion.org]

$$h\cos(e) = A\cos(\alpha), \tag{A1}$$

$$A\sin(\alpha) = R + h\sin(e), \tag{A2}$$

$$A\sin(\alpha) - R = A\tan(e)\cos(\alpha), \tag{A3}$$

$$\theta = \pi - 2\left(\frac{\pi}{2}\right) + 2\alpha = 2\alpha. \tag{A4}$$

Figure 13 shows the arc magnitude θ with respect to the elevation. We can see that, for usual elevations, such as 5° and 10°, the arc should be sufficiently large (70° and 90°, respectively) to have two satellites transmitting the same sequence without being seen by a receiver on Earth. In the case of Galileo HAS, we assume 10 sequences assigned to 20 satellites, where each sequence is assigned to two antipodal satellites. Ten sequences over 238 pages allow an offset of 23/24 pages between MT1 sequences. As MT1 sequences are interleaved by six MT2 pages as per Figure 7, we can guarantee no repetition for Galileo up to almost 30 seconds. Note also that these geometrical considerations only apply if there are more transmitters than sequences. Otherwise, each transmitter can be assigned to a different sequence.