# Reed Solomon Codes On Graph for DVB-SH Streaming Services

Amira ALLOUM
Alcatel-Lucent
Bell Labs-INRIA ,France
amira.alloum@alcatel-lucent.com

Bessem Sayadi
Alcatel-Lucent
Bell Labs, France
bessem.sayadi@alcatel-lucent.com

Vincent Roca
INRIA
Rhones Alpes, France
vincent.roca@inrialpes.fr

***Abstract*—Our study aims at bringing a software-based alternative for decoding Reed Solomon over the MPE-IFEC in the DVB-SH system, at the cost of a lower complexity and a good performance. The MPE-IFEC is operating in the Link layer, where the lost packets are considered as erasures. In this context, we propose to recover losses by decoding on a graph the binary image of the Reed Solomon code over a Binary Erasure Channel. Our approach is based on the recent advances in codes on graph theory, and reveals Maximum Likelihood performance.**

## I. Introduction

Multimedia Broadcasting services are usually provided over imperfect networks, where data losses are common. Upper layer FEC(Forward Error Correction) solutions are proposed to overcome the losses resilient to physical layer FEC mechanisms, and link layer retransmission schemes . At the receiver side, each packet is considered by the upper layers either completely received or completely lost based on a CRC (Cyclic Redundancy Check). Accordingly, the FEC decoder considers a virtual erasure channel.

In this context, different upper layer FEC solutions are available in several specifications for different applications. The solutions are partly integrated in the application layer above the IP level, then referred to as Application Layer FEC (AL-FEC), or in the link layer below the IP level, then referred to as Link Layer FEC (LL-FEC).

DVB standards include upper layer FEC in streaming and file delivery solutions on the application layer, as well as in link layer protocols. In each one of both layers, the FEC requirements vary. For instance, within LL-FEC the codeword length is small to moderate, in contrast with AL-FEC. Moreover, the lower the receiver complexity is, the better the streaming real time constraints would be respected.

Direct mobile reception by S-band satellites is possible thanks to the satellite/terrestrial system for broadcasting multimedia services to mobile receivers namely the DVB-SH standard. Nevertheless, a deep signal fading events lasting upto several seconds impacts negatively the quality of experience of the service. To overcome these critical conditions, a Multiple Protocol Encapsulation for Inter-Burst Forward Error Correction(MPE-IFEC) is introduced.

The MPE-IFEC is dedicated to cope with the impairments of the satellite propagation channel via a specific combination of interleaving and LL-FEC protection. The Sliding Reed Solomon Encoding (SRSE) is one of the MPE-IFEC mapping incorporated into the DVB-SH implementation guidelines [1].

In actual fact, Reed Solomon codes are attractive for their optimal erasure recovery capacity. Nevertheless, they require a dedicated chipset to support their complex algebraic decoding dealing with polynomials in finite fields. To overcome this practical inconvenient, some software-based implementations have been proposed by [2]. However, these approaches still demanding in CPU processing and dealing with finite fields operations.

In order to obtain a low complexity software-based MPE-IFEC decoding solution for the DVB-SH, we propose to investigate decoding Reed Solomon codes using codes on graphs approaches and the related low complexity sum-product algorithm. These approaches allow circumventing the complexity of finite fields operations by operating over a sparse graph representation of the binary images of the Reed Solomon codes [3], [4].

In our setting, we investigate the decoding of Reed Solomon codes on graph over the Binary Erasure Channel (BEC), by extending an iterative decoding approach based on adapting the parity check matrix and previously proposed for the AWGN and Fading channels in [3], [4]. Then, we propose to compare our simulations results to the maximum likelihood performance of the binary RS construction [5], and the improved sphere packing bound recently proposed in [6]. The design of such decoding approaches aims at enhancing the existing upper layer FEC solutions , and striking a balance between complexity and decoding capability of Reed Solomon codes.

The paper is organized as follows. In section II, we describe the considered DVB-SH MPE-IFEC system model ,and introduce the related notations. In section III, we discuss several properties of the binary Reed Solomon codes and evaluate analytically the averaged performance of the maximum likelihood (ML) decoder. In section IV, the adaptive parity check matrix (ADP) based sum-product decoding algorithm is described for the special instance of the BEC. In section V simulation results of the ADP sum-product algorithm over the BEC, are presented and compared with the algebraic hard decoding Berlekamp Massey algorithm, then also with some theoretical bounds. Finally, conclusions are given in section VI.

## II. System Model and Notations

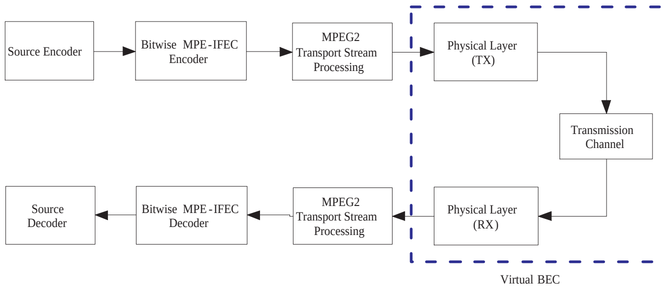


Fig. 1. Proposed System Model for the DVB-SH Standard.

In the DVB-SH system, MPE-IFEC is based on a specific data and redundancy interleaving coupled to Reed-Solomon. As depicted in Figure (1), the IP packets are processed by the MPE-IFEC to generate data and parity sections. These later are transported on MPEG-2 transport stream, then provided to the physical layer. At the receiver side, each packet is considered by the upper layers either completely received or completely lost based on a CRC (Cyclic Redundancy Check). Accordingly, the FEC decoder considers a virtual erasure channel.

In our setting we assume that the MPE-IFEC frame is bitwise. Consequently, the erasures occur following the binary Erasure channel model (BEC). Hence, we focus on the communication system depicted in Figure (2).

Let $\mathbf{x} = x_1^k = (x_1, x_2, ..., x_k)$, where $x_i \in \{0,1\}$ be a bit sequence of length $k$ supplied to the MPE-IFEC encoder, supposed to be independant, identically and uniformly distributed. The sequence $\mathbf{x}$ is encoded by the binary image of an $(N, K)$ Reed Solomon code over $GF(2^m)$ of rate $R = K/N = k/n$ into the code sequence $\mathbf{c} = (c_1, c_2, ..., c_n)$ of length $n > k$. Let us recall that $K = k/m$ and $N = n/m$, are the length of the information word and the codeword respectively at the symbol level. The $(N-K) \times N$ parity check matrix over $GF(2^m)$ can be represented as follows:

$$\mathbf{H_s} = \begin{pmatrix} 1 & \beta & ... & \beta^{(N-1)} \\ 1 & \beta^2 & ... & \beta^{2(N-1)} \\ & & ... & \\ 1 & \beta^{(N-K)} & ... & \beta^{(N-K).(N-1)} \end{pmatrix}$$

where $\beta$ is the primitive element in $GF(2^m)$. The matrix $\mathbf{H_s}$ has different binary image expansions parity check matrices of dimension $(n-k) \times n$ (see [7] for details).

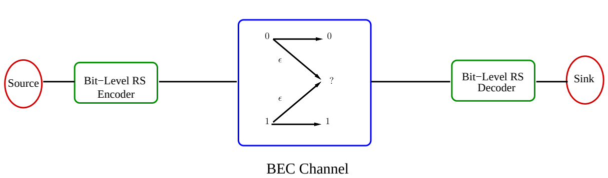


Fig. 2. Communication System Model.

In our setting we consider $\mathbf{H_b}$ as one of those binary image expansions and its related generator matrix to encode the binary sequence $\mathbf{x}$. The codeword $\mathbf{c}$ is transmitted over a BEC channel, then received as the noisy vector $\mathbf{y} = (y_1, y_2, ..., y_n)$. $y_i$ denotes the binary channel output and takes its values in the set $\{0, 1, ?\}$, where $y_i =?$ denotes the observed erasures. Let us denote $\epsilon$ as the channel erasure probability, where the direct channel observation is written as:

$$obs(x_i) = p(y_i|x_i) = \begin{cases} 1-\epsilon & \text{if } y_i = x_i \\ 0 & \text{if } y_i = \overline{x_i} \\ \epsilon & \text{if } y_i =? \end{cases}$$

The decoder that receives an erased codeword $\mathbf{y}$, estimates $\mathbf{x}$ utilizing a sum-product algorithm over a factor graph equivalent to the one associated to the binary parity check matrix $\mathbf{H_b}$ [8].
In all the following , we consider the log likelihood ratio (LLR) notation, in order to describe the reliabilities flowing through the bipartite graph related to the sum-product algorithm. Hence, the LLR describing the channel observation becomes:

$$LLR_{obs}(y_i) = \log\left(\frac{p(y_i|x_i=0)}{p(y_i|x_i=1)}\right) = \begin{cases} \infty & \text{if } y_i = 0 \\ -\infty & \text{if } y_i = 1 \\ 0 & \text{if } y_i =? \end{cases}$$

## III. The Binary Reed Solomon Codes and Their Maximum Likelihood Performance

In the case of a binary linear code, a maximum-likelihood decoder over the BEC fails to recover a given erasure pattern if and only if this pattern contains the support of (at least one) nonzero codeword. Hence, we assume that the all zero codeword is transmitted. Then, the analysis depends on the number of binary codewords within a certain Hamming distance from the all zero codeword, namely the binary weight enumerator (BWE) of the code.

Let $E(w)$ denotes the number of codewords with the weight $w$ and $db_{min}$ denotes the minimal distance of the binary code. Hence, the analytical expression of the decoding failure probability of the Maximum Likelihood decoder is written as:

$$P_{ML}(\epsilon) = \sum_{w=db_{min}}^{n} E(w)\epsilon^w(1-\epsilon)^{(n-w)} \quad (1)$$

The symbol-level weight distribution of the Reed Solomon over $GF(2^m)$ is well known [5]. Whereas, the bit-level weight enumerator of a binary Reed Solomon code is not unique, and depends on the specific basis used to represent the symbols in $GF(2^m)$ as bits. This is making the bit-level BWE given a special basis, difficult to obtain analytically. Moreover, this fact reveals that every binary Reed solomon code, is a specific code with a fixed rate and dimension, but a different BWE and minimum distance.

In this respect, Retter [9], then El khamy *et.al* [5] have computed the averaged weight enumerator over the average ensemble of an RS code, taken by averaging over all possible binary expansions. The average ensemble of Reed Solomon is also called Generalized RS ensemble (GRSE).

The derived expressions have been used in the literature to evaluate bounds on the Maximum Likelihood performance for different bit-level hard and soft decoders. Hence, in order to evaluate the average Maximum Likelihood performance of the GRSE over the BEC, we just have to replace the BWE expressions given in [5] in the equation (1).

Moreover, It has been shown in [5] that the generalized Reed Solmon codes are good codes, with an asymptotically good minimum distance that is always greater than the minimum distance of the symbol-level Reed Solomon. In addition, it has been proved that as the code length and the field size grow, the average binary Reed Solomon behaves as a random code of the same dimensions. This result would be confirmed further through our simulations results.

## IV. The Adaptive Parity Check Matrix Based Sum-Product Algorithm for the BEC

The adaptive Parity Check Matrix (ADP) based sum-product Algorithm, has been proposed for the first time in [3] for decoding iteratively binary Reed Solomon codes over AWGN and Rayleigh fading channels.

The sum product algorithm, is performing well over sparse factor graphs. Nevertheless, the bi-partite graph corresponding to the binary parity check matrix $\mathbf{H_b}$ is too dense to support a message passing algorithm. Therefore, the ADP sum-product algorithm circumvents this inconvenient, by eliminating cycles within the subgraph corresponding to the low reliability received bits.

In the special case of the BEC, the values of the initial LLRs are reduced to three values $\{-\infty, 0, \infty\}$. Hence the ADP-algorithm, eliminates stopping sets, only within the subgraph containing erasures.
The complete algorithm is described as in the following:

---

**Algorithm:** ADP based Sum-Product Algorithm for the BEC.

---

- **Step 1** : Initialization:
  Initialize the LLR's for the observed coded bits from the channel $LLR_{obs}(y_i) \in \{-\infty, 0, \infty\}$.
- **Step 2** : Parity Matrix Adaptation:
  1) Order the LLR values in increasing reliability using the absolute LLR values $|LLR(y_i)|$.
  2) Apply Gaussian Elimination to systemize the $(n-k)$ independant columns corresponding to the erased positions. $\mathbf{H_b}$ becomes $\hat{\mathbf{H}}_b$.
- **Step 3** Sum Product Algorithm:
  Apply the Sum Product algorithm over the factor graph corresponding to $\hat{\mathbf{H}}_\mathbf{b}$.
- **Step 4** Termination Step:
  If there are not remaining erasures , terminate the algorithm, otherwise declare a failure.

---

In our context, no damping coefficient is used in the sum-product algorithm, and none of the proposed graph optimization in the original algorithm (in [3]) needs to be considered. We find out that the algorithm doesn't require more than one iteration to converge or fail. This is making the complexity decreasing in comparison with the original algorithm performing multiple Gaussian eliminations.

## V. Simulations and Results

In the present section, simulation results for ADP-based sum-product decoding of binary RS codes are presented with their related theoretical bounds.

The following notations will be used in the legends. ADP denotes the ADP-based sum product decoding algorithm described in section (IV). BMA denotes the Berlekamp Massey algorithm, that is the symbol-level bounded distance decoding algorithm, considered in the actual DVB-SH standard. The ML bound, denotes the averaged maximum likelihood decoding performance computed using the equation (1) and the averaged BWE expressions given in [5].

Following these notations, we first compare the performance of the ADP-sum product decoder, to the bit-level average ML performance for the $(7, 5)$ RS code in Figure (3). The curves reveal that the ADP-sum product algorithm performs as good as the average ML decoder of the GRSE over the BEC. This has been predicted theoretically in [3], through the geometric interpretation of the ADP based sum-product algorithm.

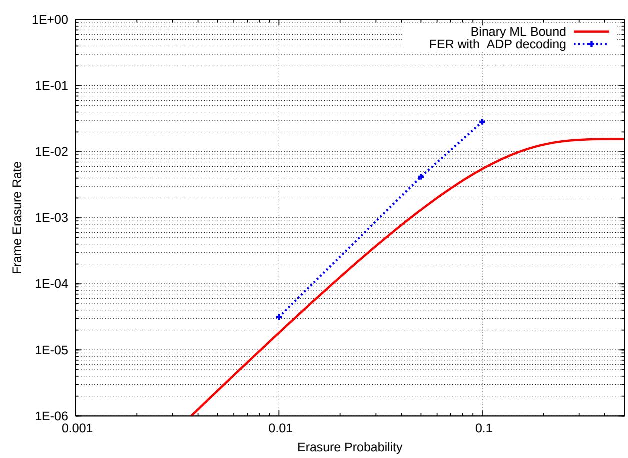


Fig. 3. Comparaison of the simulated ADP decoding performance with the Maximum Likelihood Bound for the Reed Solomon (7,5).

In Figures (4) and (5), we compare the performance of the bit-level ADP-sum product decoding with the symbol-level Berlekamp Massey Algorithm in the case of the $(31, 25)$ RS code, and the $(255, 191)$ RS code of the DVB-SH standard. Both simulations reveal that the ADP-sum product algorithm outperforms the Berlekamp Massey, and recovers within $10\%$more erasures.

These results show that the symbol-level bounded distance decoding algorithms widely used in practical systems, don't fully exploit the error correction capability of the RS codes.

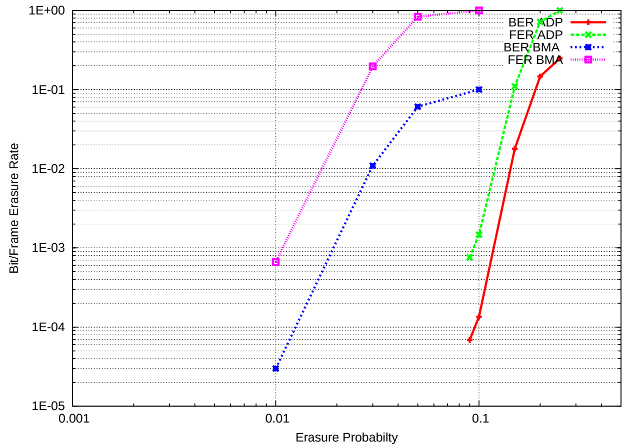


Fig. 4. Performance of the Reed Solomon Code (31,25) over the BEC.

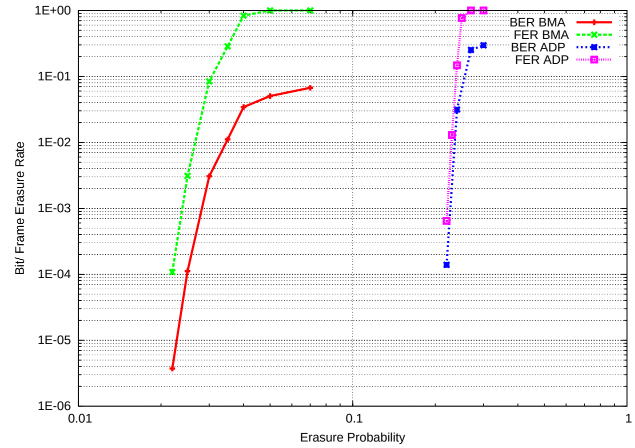


Fig. 5. Performance of the Reed Solomon Code (255,191) over the BEC.

Those can be decoded far beyond the minimum distance using bit-level decoding algorithms.

In Figure (6), we compare the simulated ADP sum-product performance to the improved sphere packing bound recently proposed for the BEC channel in [6] , for codes of Rate $R = 0.75$ and length $N = 2048$, which meets the properties of the standard $(255, 191)$ RS code. The simulated curve approaches the sphere packing bound within $2\%$. This result, means that the binary $(255, 191)$ RS code is itself a good code.

We have also plotted, the exact decoding error probability of random binary linear block code under ML decoding, also proposed in [6], for codes of Rate $R = 0.75$ and length $N = 2048$. We can observe that the curve is superimposed with the ADP-sum product decoding simulated curve of the $(255, 191)$ RS code.

Our results , meet those theoretically proven in [5] claiming that as the code length and the field size grow, the binary images of Reed Solomon behave as a random code of the same dimensions, and that the Generalized Reed Solmon codes are good codes, with an asymptotically good minimum distance.

## VI. Conclusion

We conclude that over the BEC, the ADP-sum product algorithm, provides a better performance at the cost of lower complexity compared to the Berlekamp Massey algorithm.

We have shown that the $(255, 191)$ RS code of the DVB-SH standard is a good code, almost attaining the sphere packing bound within $2\%$. Moreover, the ADP sum-product decoding is able to be software implemented, in the DVB-SH standard.

Our results reveal that it is of practical value to use bit-level decoding algorithms for the Reed Solomon codes, since the symbol-level bounded distance decoding algorithms widely used in practical systems, doesn't fully exploit the error correction capability of the code. Our study can be straightforwardly extended to the DVB-H standard.

## VII. Acknowledgment


The work is funded by the common laboratory between Alcatel-Lucent Bell-labs France and INRIA.


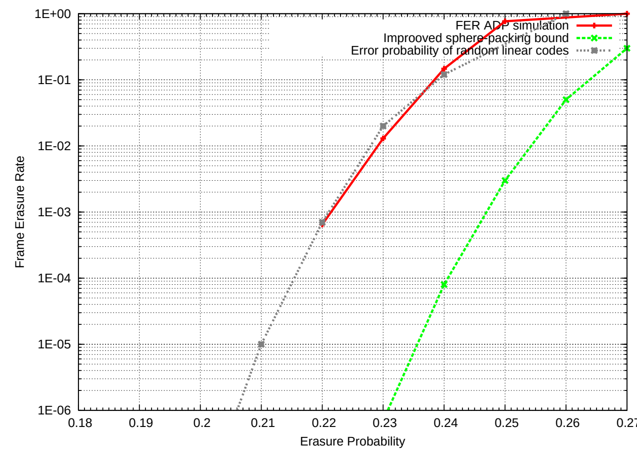


Fig. 6. Performance of the RS Code (255,191) over the BEC compared to the Sphere Packing lower Bound and the exact decoding error Probability of random binary linear block under ML decoding for $N = 2040$ and $R = 0.75$.

## References


[1] European Telecommunications Standards Institute, "Digital video broadcasting (DVB); DVB-SH implementation guidelines," Tech. Rep., Draft TS102 585 V1.1.1, May. 2008.

[2] L. Rizzo, "Effective erasure codes for reliable computer communication protocols," *ACM SIGCOMM Computer Communication Review*, vol. 27, no. 2, pp. 24–36, 1997.

[3] J. Jiang and KR Narayanan, "Iterative soft decision decoding of Reed Solomon codes based on adaptive parity check matrices," in *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*.

[4] A. Ahmed, R. Koetter, and NR Shanbhag, "Performance analysis of the adaptive parity check matrix based soft-decision decoding algorithm," in *Signals, Systems and Computers, 2004. Conference Record of the Thirty-Eighth Asilomar Conference on*, 2004, vol. 2.

[5] M. El-Khamy and R.J. McEliece, "Bounds on the average binary minimum distance and the maximum likelihood performance of Reed Solomon codes," in *42nd Allerton Conf. on Communication, Control and Computing*, 2004.

[6] G. Wiechman and I. Sason, "An improved sphere-packing bound for finite-length codes over symmetric memoryless channels," *IEEE Transactions on Information Theory*, vol. 54, no. 5, pp. 1962–1990, 2008.

[7] S. Lin and D.J. Costello, *Error control coding: fundamentals and applications*, Prentice Hall, 1983.

[8] F.R. Kschischang, B.J. Frey, and H.A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Transactions on information theory*, vol. 47, no. 2, pp. 498–519, 2001.

[9] CT Retter, "The average binary weight-enumerator for a class of generalizedReed-Solomon codes," *IEEE Transactions on Information Theory*, vol. 37, no. 2, pp. 346–349, 1991.