Algebraic Soft-Decision Decoding of Reed-Solomon Codes with Erasures on Gaussian Channels

Fábio Rizental Coutinho and Evelio Martín García Fernández

***Abstract*— The search for increasing the error performance of algebraic soft-decision decoding of high rate Reed-Solomon (RS) codes motivates the development of this work in an attempt to determine the ultimate error-correcting capabilities of algebraic soft-decision decoding of RS codes in Gaussian channels with erasures. It is shown through simulation that a significant performance improvement can be obtained when the unreliable bits received from channel output are declared as erased bits. An alternative method to construct the reliability matrix is developed through the mapping of the a posteriori channel probabilities in order to assign equal multiplicity for symbols with the same erased bits patterns. Conversely, it is also shown through simulation that trying to declare the unreliable symbols received from the channel as erasures does not lead to any performance gain and in some cases it would affect the decoder performance.**

***Index Terms*— Reed-Solomon codes, algebraic soft-decision decoding, erasure channels, error correcting codes.**

To be reviewed as a Regular paper in Coding Theory and Techniques

I. Introduction

Reed-Solomon codes [1] are among of the most important error correcting codes which are widely employed in many digital communications and data storage systems with applications ranging from digital data storage (CD and DVD), to satellite communication systems. One of the most important research subject about Reed Solomon codes has been to achieve soft decision decoding throughout its strongly algebraic nature in contrast with the traditional approach of using an (unpractical) trellis representation of the codes. In 1999, Guruswami and Sudan showed in [2] how they surpassed the conventional error correction capacity of $(n-k)/2$ symbols through a polynomial-time list decoding algorithm that corrects up to $n-\sqrt{nk}$ symbol errors. To achieve this results they thought the decoding process as if it was a problem of constructing a bivariate polynomial that pass through all the points received from the channel with an arbitrary order or multiplicity m. For a comprehensive tutorial on the Guruswami-Sudan (GS) decoding algorithm we recommend [3] and [4]. Lately, Koetter and Vardy, in [5], adapted the strongly algebraic structure proposed in [2] to reach a major breakthrough in this research area: soft decision decoding of Reed-Solomon codes. They showed that, instead of choosing a fixed interpolation multiplicity for all points, the interpolation multiplicity m could be arbitrarily changed for each point considering the soft information available for them. They also showed that for codes of infinite length the best way to choose the value of m is by making it proportional to the soft information available for each point. In [6], [7] and [8] there were presented some multiplicity assignment strategies which were optimized for infinite-length codes through complex numeric algorithms. However for codes of finite length, an optimum multiplicity assignment strategy is still an open problem.

An erasure is an error whose location is known but its value is unknown. Erasures can occur when the signal received from the channel is simply lost or when it was so corrupted that the receiver cannot decide anything about it; in these cases the received symbols are declared as erasures. In [9] the decoding radius when using algebraic soft-decision decoding (ASD) over the binary symmetric channel (BSC) and the binary erasure channel (BEC) were investigated and it was shown that, for those kind of channel models, the proportional multiplicity assignment strategy is optimum. The authors also showed how ASD can improve the performance of the conventional Berlekamp-Massey decoding algorithm over erasure channels.

In an attempt to improve the performance of algebraic soft-decision decoding of finite length, high rate RS codes without increasing the decoding complexity, this paper presents an alternative method for constructing the reliability matrix based on the erasure of unreliable bits by considering them equally probable. The validity and decoding performance obtained by the proposed method were confirmed through simulation. The method is extended by erasing unreliable symbols from the channel, however in this case the decoder performance was affected due to the great number of possibilities that exist when a symbol is declared as an erasure.

The organization of the paper is as follows. In section II the proposed method for mapping the reliability matrix by intentionally erasing the unreliable bits and assigning the same a posteriori probabilities to symbols with equal bit erasure patterns are described. Simulation results are shown in section III. Conclusions and future works are drawn in section IV.

Fábio Rizental Coutinho is with Electrical Engineering Department, Federal University of Paraná, Centro Politécnico, P.O. Box 19011, 81531-970, Curitiba, PR, Brazil, fabio.rizental@perkons.com.br, Tel. +55-41-35443246, Fax +55-41-33613228

Evelio Martín García Fernández is with Electrical Engineering Department, Federal University of Paraná, Centro Politécnico, P.O. Box 19011, 81531-970, Curitiba, PR, Brazil, evelio@eletrica.ufpr.br, Tel. +55-41-33613221, Fax +55-41-33613228

ISSN 1980-6604/$20.00 © 2007 SBrT/IEEE

II. Background

In this section some background concepts on Reed-Solomon codes and algebraic soft-decision decoding of RS codes that are relevant to this paper are reviewed.

A. Classic Construction of Reed-Solomon Codes

Consider an (n, k) RS code with length n and dimension k, constructed over a Galois field with q elements, $\mathbb{F} = GF(q)$. Let α be a primitive element in GF(q). The message to be transmitted consists of k elements of GF(q) that defines a message vector $\mathbf{m} = (m_0, m_1, ..., m_{k-1}) \in GF(q)^k$, that can also be used to construct a message polynomial $m(x) = m_0 + m_1 x + ... + m_{k-1}x^{k-1} \in GF(q)[x]$ with degree at most $k-1$. A RS (n, k) code maps the message polynomial $m(x)$ into a codeword vector $\mathbf{c} = (c_0, c_1, ..., c_{n-1})$ with n elements, through the evaluation of $m(x)$ at all non-zero elements of GF(q) as:

$$(c_0, c_1, ..., c_{n-1}) \triangleq (m(\alpha^0), m(\alpha^1), ..., m(\alpha^{n-1})). \qquad (1)$$

It can be noticed that the construction process of RS codes as showed above is a linear process. It also can be noticed that, being k and n, respectively, the dimension and the length of the code, the minimum distance can be found by using the property of fundamental algebra that a polynomial of degree less than k can has up to $k-1$ zeros, so it can be at most $n-(k-1)$ non-zero symbols in an RS codeword, which define its minimum distance: $d_{min} = n-k+1$, so RS codes are maximum distance separable (MDS) codes. Hence, each codeword of a Reed-Solomon (n, k) code consists of some n values of a polynomial $f(x)$ of degree less than k. And this polynomial can be uniquely recovered by interpolation from any k of its values. Thus an RS(n, k) code can correct up to $n-k$ erasures or, equivalently, up to $(n-k)/2$ symbol errors.

B. Algebraic Hard-Decision Guruswami-Sudan Decoding Algorithm

Guruswami and Sudan showed in [2] that much more errors can be corrected by using a stronger algebraic structure in the decoder algorithm and by changing the conventional bounded distance decoding paradigm to a list decoding procedure.

It was already pointed out that the RS codewords can be thought as polynomials of degree less than k. As a consequence, a transmitted RS codeword can be viewed as an algebraic curve of the form $y - f(x)$, with maximum degree $k-1$. The GS list decoding algorithm for RS codes considers the RS codewords as bivariate curves and is based on the Bézout's Theorem that estipulate,

Theorem 2.1: Two algebraic curves of degrees d and δ intersect in $d\delta$ points, and cannot meet in more than $d\delta$ points unless the equations defining them have a common factor.

Therefore, if it could be constructed a bivariate polynomial curve $Q(x, y)$ that intercepts the points received at the channel output in more points than the product of the degrees of $Q(x, y)$ and $y - f(x)$, then by Theorem 2.1, this constructed curve and the polynomial representing the transmitted codeword must have a common factor and as the transmitted polynomial is prime, the only way for the two curves to have a common factor is $y - f(x)$ being a factor of $Q(x, y)$.

Formally, consider a bivariate polynomial with coefficients over a GF(q):

$$Q(x, y) = \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} a_{i,j} x^i y^j \in GF(q)[x, y]. \qquad (2)$$

Let w_x and w_y be two non-negative real numbers, so the weighted degree (w_x, w_y) of $Q(x, y)$ can be defined as the maximum $iw_x + jw_y$ which makes $a_{i,j} \neq 0$. Let α, β be elements of GF(q), so the Hasse's derivative of $Q(x, y)$ at points $(\alpha, \beta) \geq 0$ is defined by:

$$Q_{r,s}(x, y) = \sum_i \sum_j \binom{i}{r}\binom{j}{s} a_{i,j} x^{i-r} y^{j-s}. \qquad (3)$$

Hence $Q(x, y)$ pass through the points (x_i, y_i) with multiplicity m_i if $Q_{r,s}(x, y) = 0$, for all $\alpha + \beta < m_i$.

Consider a received word as being $y = c + e$ where e is the error vector introduced by the channel. An element x_i over GF(q) can be associated with y_i defining a set of n points $(x_1, y_1), (x_2, y_2), ..., (x_n, y_n)$. If there is no channel noise ($e = 0$) then $y_i = f(x_i)$ and the polynomial $Q(x, y) = y - f(x)$ pass through all the n points with multiplicity one. In the presence of noise ($e \neq 0$), the interpolating polynomial will pass through some points that do not belong to the transmitted codeword. The Guruswami-Sudan algorithm guarantees that the transmitted codeword will be in $Q(x, y)$ if the number of coefficients of the interpolating polynomial do not exceed the number of constraints:

$$\left(\sum_{j=1}^{n} m_i(m_i+1)/2\right) < C(v, l), \qquad (4)$$

where $v = k-1$ and $C(v, l)$ is the number of monomial of weighted degree $(1, v)$ less than or equal to l which is described by:

$$C(v, l) = \left(\left\lfloor \frac{l}{v} \right\rfloor + 1\right)\left(l + 1 - \frac{v}{2}\left\lfloor \frac{l}{v} \right\rfloor\right). \qquad (5)$$

The Guruswami-Sudan decoder is a list decoding algorithm based on interpolation and consist of two main steps:

1) Interpolation: Given a set of points $P = \{(x_1, y_1), (x_2, y_2), ..., (x_n, y_n)\}$ over GF(q)×GF(q) and a positive integer m, find a bivariate polynomial $Q_P(x, y)$ of minimum $(1, k)$ weighted degree, that pass through all the points of P with multiplicity at least m.
2) Factorization: Given a bivariate polynomial $Q_P(x, y)$, find all the factors of $Q_P(x, y)$ of the form $y - f(x)$ with degree $f(x) < k$.

C. Algebraic Soft-Decision Decoding

An algebraic soft-decision decoder makes use of the soft information received from the channel, which is available in many situations [10], [11]. This information are generally delivered as a $q \times n$ reliability matrix Π which relates the a posteriori probability of each symbol from GF(q) with its position in the codeword vector. For an RS code, a random codeword $X = (x_1, x_2, ..., x_n)$ is selected to be transmitted and at the output of the memoryless channel an observation vector $Y = (y_1, y_2, ..., y_n)$ is constructed. If it is assumed like in [5] that all the elements of X are independent and uniformly distributed over GF(q), the a posteriori probabilities can be defined as,

$$\pi_{i,j} = P(x_j = \alpha_i | y_j),\ i = 1, 2, ..., q, j = 1, 2, ..., n. \quad (6)$$

Therefore the reliability matrix Π can be constructed using the entries $\{\pi_{i,j}\}$ as computed in (6), where the set $\{\alpha_1, \alpha_2, .., \alpha_q\}$ are all the elements of GF(q).

Once obtained the reliability matrix Π, a multiplicity assignment algorithm computes a $q \times n$ multiplicity matrix M of non negative integers. In [5] it was shown that the optimum multiplicity assignment strategy for Gaussian channels is to make the multiplicity matrix M proportional to the reliability matrix Π as

$$m_{i,j} = \lfloor \lambda \pi_{i,j} \rfloor, \quad (7)$$

where λ is an arbitrary non-negative real number. The proportionality constant λ controls the tradeoff between performance and complexity of the decoder so it must be carefully chosen according to the code used.

The number of linear constraints or cost of interpolation associated with the multiplicity matrix M is defined in [5] as,

$$|M| \triangleq \frac{1}{2} \sum_{i=1}^{q} \sum_{j=1}^{n} m_{i,j}(m_{i,j} + 1), \quad (8)$$

and the score of a codeword vector **c** is defined with respect to a given multiplicity matrix M as:

$$S_M(\boldsymbol{c}) \triangleq \sum_{i=0}^{n-1} M_i(c_i). \quad (9)$$

The score thus represents the total multiplicity of all the points associated with the vector **c**. This matrix is then passed to a modified Guruswami-Sudan algorithm that will perform the two final steps of the decoding process.

Consider a bivariate polynomial over GF(q), $Q(x, y) = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} a_{i,j} x^i y^j$. Let w_x and w_y be two non negative real number, so the weighted degree (w_x, w_y) of $Q(x, y)$ could be defined as the maximum $iw_x + jw_y$ such that $a_{i,j} \neq 0$.

The first step is the soft interpolation that consists of constructing a bivariate polynomial $Q(x, y)$ of minimal $(1, k-1)$ weighted degree that passes through each of the points (x_j, α_i) with multiplicity $m_{i,j} \neq 0$, for $i = 1, 2, ..., q$ and $j = 1, 2, ..., n$.

The second step, is the factorization, that consists of finding all the factors of the form $(y - f(x))$ that divide $Q(x, y)$, where $f(x)$ is a polynomial of degree less than k. Each polynomial $f(x)$ obtained in this step will be in the list of possible transmitted codewords.

Although the performance of the ASD decoder is difficult to compute and characterize, it is shown in [5] that a sufficient condition for ASD to return the transmitted codeword as the cost $|M| \to \infty$ is:

$$S_M(\boldsymbol{c}) > \sqrt{2(k-1)C_M}. \quad (10)$$

For finite interpolation cost the sufficient condition of (10) is well approximated by [7]:

$$S_M(\boldsymbol{c}) > \left\lfloor \sqrt{2(k-1)C_M} - \frac{k-1}{2} \right\rfloor. \quad (11)$$

The precise characterization of the performance bounds of the Koetter-Vardy algorithm [5] is denominated the asymptotic performance and is given by:

$$\frac{\langle \Pi, [\boldsymbol{c}] \rangle}{\sqrt{\langle \Pi, \Pi \rangle}} \geq \sqrt{k-1}. \quad (12)$$

D. Performance Analysis of ASD over the Binary Erasure Channel

Consider Reed-Solomon codewords over GF(2^m) whose symbols are being transmitted as binary m-tuples through a BEC channel with erasure probability p. In this model of discrete memoryless channel the transmitter can only send one bit at a time, '0' or '1', but at the receiver side either could be a '0', a '1' or a message saying that the bit was not received, which means that the bit was erased or simply that an erasure has occurred. The binary erasure channel is characterized by an erasure probability p, an input random variable X that can take values from the alphabet $\{0, 1\}$ and an output random variable Y with values from the alphabet $\{0, 1, e\prime\}$, where $e\prime$ is the erasure symbol. Therefore the channel transition probabilities can be described as shown in Figure 1 where the symbol '?' denotes the erasure sample value of Y.

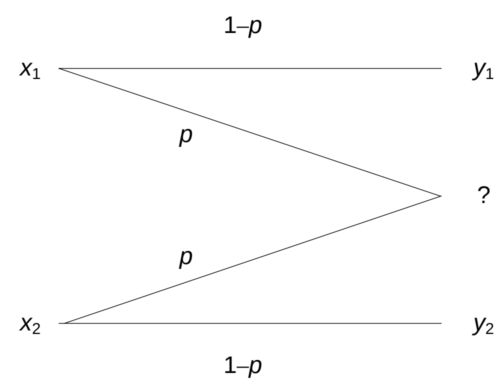

Fig. 1. Transition Probability Diagram for the Binary Erasure Channel

When performing the ASD decoding process, if an erased bit exists in an m-bit symbol, then when the multiplicity assignment step is reached and taking into account that the a posteriori probability values are not available to the decoder, it must be considered that the two candidate symbols (one with the erased bit represented as '0' and the other as '1') are equally probable. And as in [5], [9], [8] it will be considered here that the codeword symbols are equiprobable, so there is no preference of one symbol over another. Hence it can be assigned the same multiplicity for two candidate codewords that are equiprobable.

Furthermore it will be defined, as in [9], a symbol of type i as being a symbol that has i erased bits. For a Reed-Solomon code over GF(2^m), it can be up to $m+1$ different symbol types. Let the number of symbols of type i in a received codeword be a_i [9]. As mentioned before, we will assign equal multiplicity to symbols of the same type, so the multiplicity for a symbol of type i is m_i. Therefore the total assigned multiplicity for a symbol of type i will be $2^i m_i$. The score and cost of the multiplicity matrix will be, respectively,

$$S = \sum_{i=0}^{m} a_i m_i, \tag{13}$$

$$C = \sum_{i=0}^{m} a_i 2^i \binom{m_i+1}{2}. \tag{14}$$

For larger values of m_i, (14) can be approximated by [9]:

$$C = \frac{1}{2}\sum_{i=0}^{m} a_i 2^i m_i^2. \tag{15}$$

Equation (10) characterizes the condition for the ASD algorithm to have success in decoding. Without loss of generality, this result can be used to find the optimum multiplicity assignment strategy for BEC channels. Consequently, the problem to be solved is to maximize the score with the cost restriction of the multiplicity matrix M. Considering high multiplicity values this problem can be expressed as,

$$max_{m_i} \sum_{i=0}^{m} a_i m_i, \tag{16}$$

subject to

$$C = \frac{1}{2}\sum_{i=0}^{m} a_i 2^i m_i^2. \tag{17}$$

This problem of optimization was solved in [9] using Lagrange multipliers and the final result was

$$m_i \propto 2^{-i}. \tag{18}$$

Hence, it can be observed that the optimum multiplicity assignment strategy for BEC channels is the assignment proportional to the reliability matrix Π.

III. Alternative Method for Mapping the Reliability Matrix

In this section it will be shown how the coding gain can be improved by means of a new method of mapping the reliability matrix.

A. Binary Symmetric Channel with Erasures

In the discrete channel model of Figure 1, all the possible errors are being treated as erasures. If the error transition probabilities were introduced in this diagram, an hybrid channel model will have been formed which is known as Binary Symmetric Channel with Erasures. In this kind of channel model two type of symbols can be transmitted, $\{x_1, x_2\} = \{0, 1\}$, and the channel output can be one of the symbols $\{y_1, y_2, ?\} = \{0, 1, e\prime\}$, depending on the channel transition probabilities. This channel model is illustrated in Figure 2.

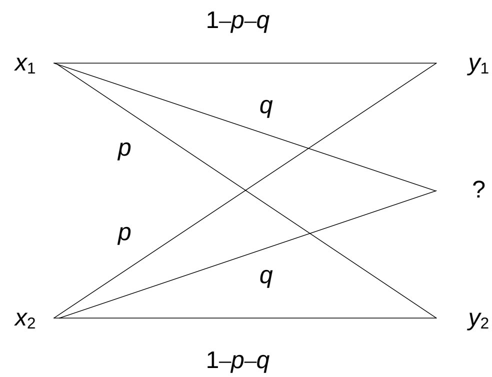

Fig. 2. Transition Probability Diagram for the Binary Symmetric Channel with Erasures

In what follows, erasures will be introduced at a Gaussian channel model output in order to extend the results about the optimum multiplicity strategy obtained for Binary Erasure Channels in [9] to Gaussian channels with erasures. The modulator-demodulator system in conjunction with the additive white Gaussian noise (AWGN) channel model can be viewed as a Binary Symmetric Channel by adapting the error transition probabilities in order to make them equal to the AWGN channel a posteriori probabilities. However we still have to deal with the erasure transition probability.

B. Assigning Equal Probabilities for Symbols with the Same Erasure Bit Patterns

Consider a binary transmission system using BPSK (*Binary Phase Shift Keying*) modulation over an AWGN channel. For this case the signal constellation consist of points belonging to the set $S = \{\sqrt{E_b}, -\sqrt{E_b}\}$, where E_b is the transmitted energy per information bit. Therefore, the conditional probability densities at the channel output are given by,

$$p(r|S=\sqrt{E_b}) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{1}{2\sigma^2}(r-\sqrt{E_b})^2} \tag{19}$$

$$p(r|S=-\sqrt{E_b}) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{1}{2\sigma^2}(r+\sqrt{E_b})^2}, \tag{20}$$

where σ^2 is the noise variance and r is a sample value of the random variable that represents the channel output. Equation (19) corresponds to the binary transmission of a '1', and (20) corresponds to the binary transmission of a '0'.

If the Binary Symmetric Channel model was under consideration and so, hard decision decoding was being used, it could have simply been used, as decision threshold, the zero value output from the channel. Hence, if a signal level greater than zero is received, it will be demodulated to a binary '1', on the other hand, received signal which values are less than zero will be demodulated to a binary '0'.

Let this model be changed in order to include erasures at the channel output. To do that, two thresholds, $-t$ and $+t$, will be introduced in such a way that all received signals that fall into the interval $[-t, +t]$ will be declared as erasures. This decision context scenario is shown in Figure 3, where the conditional probability density functions were plotted for $E_b = 1$ and $\sigma = 1$.

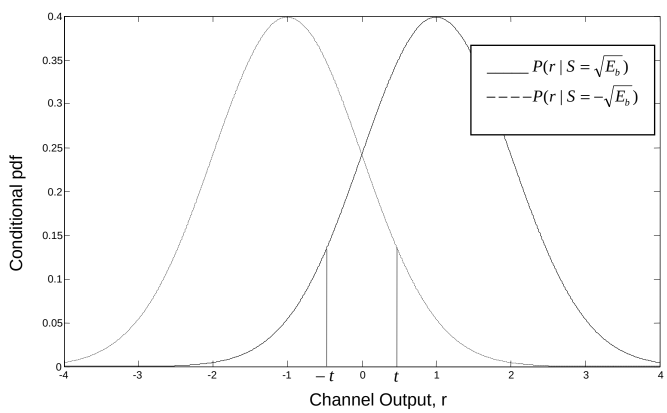

Fig. 3. Illustrating the decision problem when considering Binary Symmetric Channels with erasures

Knowing that the proportional multiplicity assignment strategy is optimum for the binary symmetric channel and for the binary erasure channel [9], and that it is asymptotically optimum for Gaussian channels [5], it can be assumed without less of generality that this assignment strategy must also be optimum for the binary symmetric channel with erasures.

Hence, as defined in subsection II-D, when there are one or more erased bits in a symbol it should be considered that all candidate symbols of being the transmitted symbol must have the same a posteriori probability and, as a consequence of using the proportional multiplicity assignment strategy, they will have equal multiplicity as well.

However the task to assign equal multiplicity based in a reliability matrix that can has symbols with erased bits is difficult. To solve this problem in an easy way we are proposing a procedure of computing the conditional probability density function at the channel output by assigning to the erased bits a value that make them having the same probability of being a '0' or a '1' in the following way,

$$p(r|S=s) = \begin{cases} \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{1}{2\sigma^2}(r+s)^2} & \text{, if } r < -t \text{ or } r > +t \\ \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{1}{2\sigma^2}(E_b)} & \text{, if } -t \leq r \leq +t \text{ ,} \end{cases} \tag{21}$$

where $s \in \{\sqrt{E_b}, -\sqrt{E_b}\}$. Assuming a memoryless channel model, it can be considered that the probability of an individual bit is independent of the probability of the previous bits, so it can be stated that the conditional probability density function of a generic m-bit symbol α from GF(2^m) is:

$$f(y|\alpha) = \prod_{i=1}^{m} p(r|S=s). \tag{22}$$

Hence, the probability of a transmitted symbol $x = \alpha$, conditioned to the observation of y at the output of the channel can be found through Bayes theorem as,

$$P(x = \alpha|y) = \frac{f(y|\alpha)}{\sum_{x \in X} f(y|x)}. \tag{23}$$

Substituting (22) into (23) and then into (6), we will be able to compute all the elements of the reliability matrix Π. Once defined the mapping between the channel output and the reliability matrix the Koetter-Vardy algorithm can be used without any modification. As a result, the points that are inside the erasure region will have the same probability which implies that, in the multiplicity assignment step, these points will have the same multiplicity which is the fundamental idea of the proposed method because a bit erasure must have the same probability of being '0' or '1'.

C. Choosing the Erasure Threshold

In order to achieve the significant coding gain that is expected when using soft decision decoding, it is important to choose an optimum erasure threshold value. Since the a posteriori probability density function has its standard deviation changed with the signal to noise ratio (SNR) at the receiver then the threshold t must vary as well. It will be defined the erasure threshold as a multiple of the standard deviation, σ, of the conditional probability density function such that,

$$t = \omega\sigma. \tag{24}$$

It can also be noticed that the standard deviation can be easily obtained through the evaluation of the SNR at the receiver. Thus, in order to find an optimum value for t, computer simulations were performed in order to evaluate the impact of varying the proportionality factor ω on the codeword error rate. As low SNR are not feasible in practice the simulation were carried out for a fixed SNR value of 6 dB. The variation of the threshold was studied for three different RS codes.

Figure 4 shows the results obtained by taking into account the RS (15, 11) code over GF(2^4), using the Koetter-Vardy soft-decision decoding algorithm and the proposed multiplicity assignment procedure on a Gaussian channel using BPSK modulation. It can be noticed that for this code there are two values that minimizes the codeword error rate: the first point is shown to be $t = 1.95$ and the second one is approximately $t = 2.80$. The second value is too large because it is not difficult to show that, with a Gaussian probability distribution, the area under the region from $r = 2\sigma$ to ∞ is only 5% of the area under the whole curve, and it was verified by simulation that 2.80 is optimum only for the specific value of SNR= 6dB, so the best choice for t is 1.95. The corresponding results when using the RS (31, 25) code over GF(2^5) are shown in Figure 5. In this case the curve converges to a minimum, so the optimum value is $t = 2.1$.

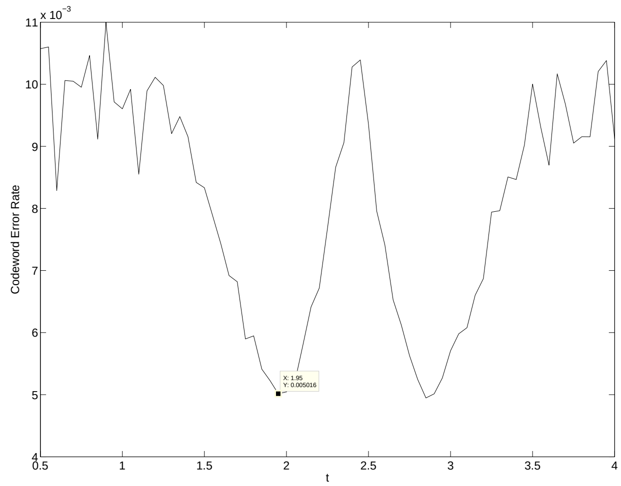

Fig. 4. Variation of the codeword error rate with the erasure threshold t for the RS (15, 11) code with BPSK modulation and bit erasures

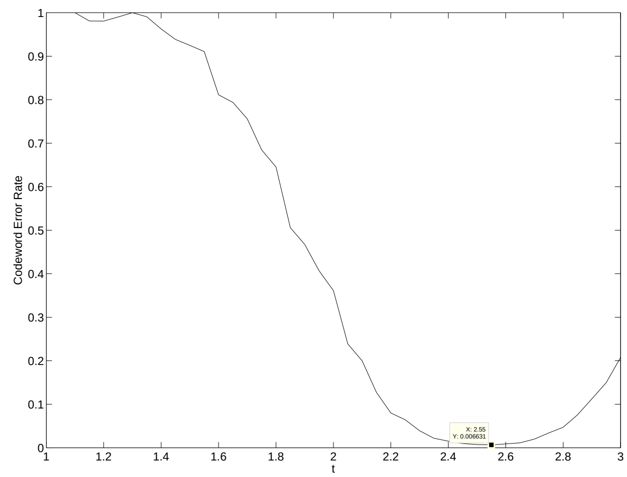

Fig. 6. Variation of the codeword error rate with the erasure threshold t for the RS (31, 25) code with BPSK modulation and symbol erasures

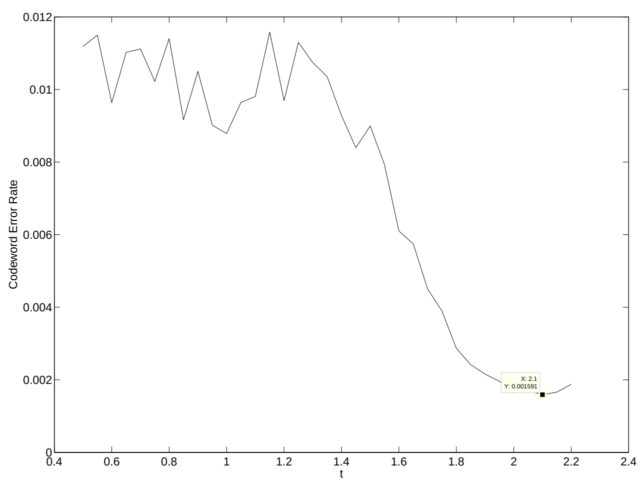

Fig. 5. Variation of the codeword error rate with the erasure threshold t for the RS (31, 25) code with BPSK modulation and bit erasures

For the case when there is a set of erased bits, which implies having symbol erasures, the threshold value was evaluated for the RS (31, 25) code using the Koetter-Vardy soft-decision decoding algorithm and the results are shown in Figure 6. Here it can be noticed that the optimum threshold value is very high, $t = 2.55$, and with this value it can be concluded that the codeword error rate will be very low, and so it will be difficult to improve the coding gain, since in this case, the existence of symbol erasures is more likely to produce decoding failures.

IV. Simulation Results

The simulation results presented in this section were obtained using the Koetter-Vardy soft-decision decoding algorithm with the proposed modification in the construction of the reliability matrix Π from the channel output in such a way that it can be assigned the same a posteriori probabilities for candidate symbols with the same bit erasure patterns. The simulations were based on the RS (15, 11) and the RS (31, 25) codes. These two codes were chosen because they are high rate and finite length codes. All the simulations were done considering an AWGN channel.

In order to make decoding performance comparisons with the Guruswami-Sudan and the Berlekamp-Welch algorithms the expressions $t_{GS} = n - \sqrt{nk}$ and $t_0 = (n - k)/2$ were used, respectively, to compute the error correction capacity associated with those algorithms. However due to the high rate of the chosen codes the performance of the Guruswami-Sudan decoding algorithm degenerates to that of Berlekamp-Welch. As Reed-Solomon codes are linear and in order to decrease the simulation run time, information vectors with all symbols equal to zero were used and then these vectors were coded and transmitted over an AWGN channel with BPSK modulation. At the channel output, hard-decision decoding was performed on the received signals in order to compute the decoding performance for the case when the Guruswami-Sudan and Berlekamp-Welch algorithms were used.

When soft-decision decoding was under consideration, it was also constructed a $q \times n$ reliability matrix Π that was used to compute the asymptotic decoding performance of the Koetter-Vardy algorithm, through equation (12), and to compute the decoding performance of the Koetter-Vardy algorithm with the proportional multiplicity assignment strategy using the parameter λ as a proportionality constant. In both cases, an unquantized AWGN channel without declaring bit erasures was considered. Another $q \times n$ reliability matrix, Π^*, was computed using the proposed method where the symbols with the same bit erasure patterns were assigned the same a posteriori probabilities using the previously computed optimum threshold t for declaring bit erasures.

Simulation results for the rate $R = 0.733$, RS (15, 11) code are shown in Figure 7. For the multiplicity assignment step it was used $\lambda = 3.99$. This value was chosen based on the results of [12], because it leads to the best decoding performance for the RS (15, 11) code. The erasure decision threshold used was $t = 1.95\sigma$. Here, at a codeword error rate of 10^{-3}, the algebraic soft-decision decoding with bit erasures provides a coding gain of about 0.3 dB when compared with the KV algebraic soft-decision decoding algorithm with $\lambda = 3.99$.

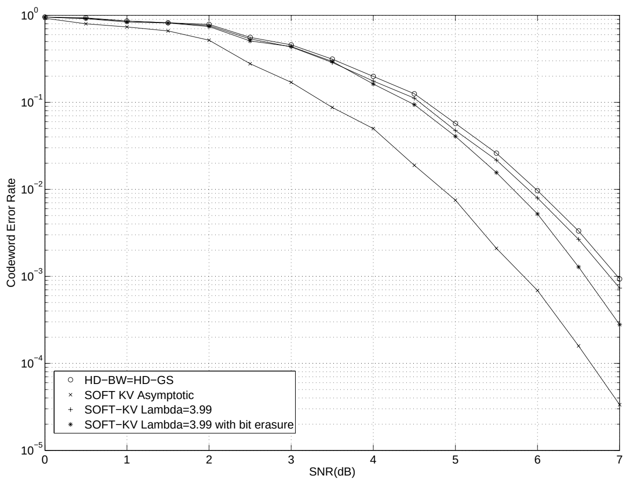

Fig. 7. Performance comparison of various decoding algorithms for the RS (15, 11) code with BPSK modulation on an AWGN channel

For the rate $R = 0.806$, RS (31, 25) code, an improvement in coding gain was achieved as shown in Figure 8. In this case, the interpolation cost used was $\lambda = 4.99$. Here it can be noticed that the curve representing the decoding performance of algebraic soft-decision decoding with bit erasures is very close to the curve representing the asymptotic performance of algebraic soft-decision decoding. Similar results have been achieved by other authors only for long codes, e.g., by using the RS (255, 239) code over GF(2^8). Another important fact is that this result was obtained using a low value for the interpolation cost, $\lambda = 4.99$, which improves the execution time of the decoding algorithm. Therefore, at a codeword error rate of 10^{-3}, the algebraic soft-decision decoding with bit erasures provides a coding gain of about 0.5 dB compared to the Koetter-Vardy ASD algorithm with $\lambda = 4.99$. The erasure decision threshold used was $t = 2.1\sigma$.

Simulation results using the Koetter-Vardy algorithm with the proposed symbol-erasure modification for the rate $R = 0.806$, RS (31, 25) code are shown in Figure 9. Again, for the multiplicity assignment step we used the interpolation cost parameter $\lambda = 4.99$. In this case the erasure symbol threshold was decreased down to $t = 2.55\sigma$. Now it can be noticed that there is a decrease in the coding gain. The reason of that behavior is that now, when a symbol is declared as an erasure, in fact what happens is that an entire column of the reliability matrix Π^*, which corresponds to the position of that symbol in the codeword, have all its entries with the same value of the a posteriori probability. As a result, the cost of the multiplicity matrix M is increased and the score of the received vector is reduced which will cause decoding failures according to equation (10).

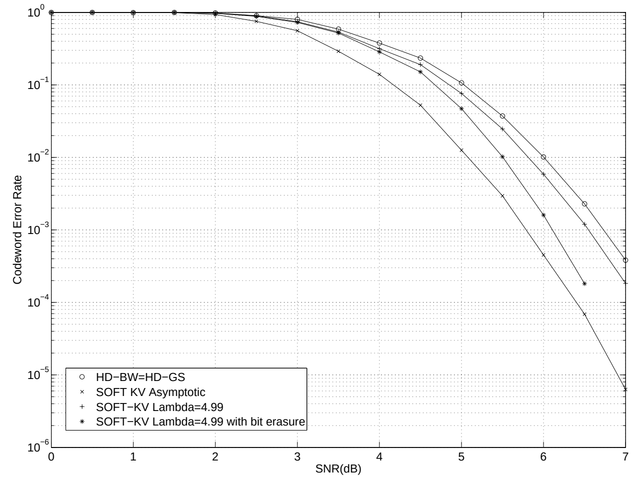

Fig. 8. Performance comparison of various decoding algorithms for the RS (31,25) code with BPSK modulation on an AWGN channel

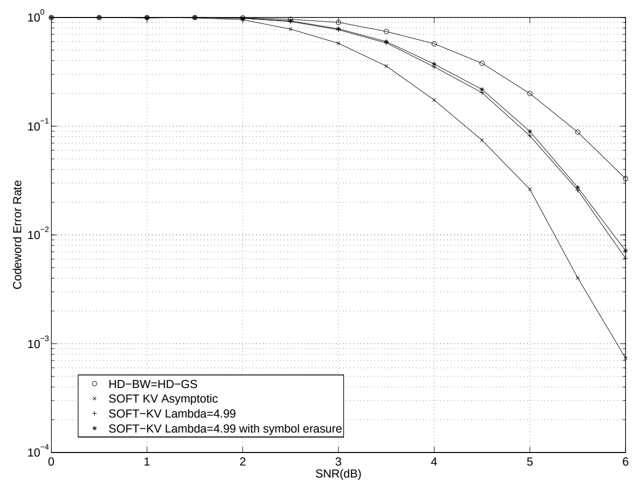

Fig. 9. Performance comparison when using algebraic soft-decision decoding with symbol erasures for the RS (31, 25) code with BPSK modulation on an AWGN channel

V. CONCLUSION

In this paper we showed that the strategy of declaring unreliable bits received from the channel output as bit erasures through an alternative mapping of the reliability matrix can be used with finite-length high-rate Reed Solomon codes in order to improve soft decision decoding performance. Results obtained with low-complexity decoding and low-cost interpolation were very close to the performance bounds promised by the Koetter-Vardy decoding algorithm. These results confirm the large potential of ASD decoding over binary channels with erasures.

On the other hand, when we tried to extend the proposed method by intentionally erasing unreliable symbols (over GF(2^m)) at the channel output we showed that it is not possible to further improve the coding gain.

There are still some open problems to be investigated. The performance analysis of ASD decoding with erasures for long codes and the use of the proposed decoded procedure in concatenated coding schemes are interesting subjects that we recommend for future works.

REFERENCES

[1] I.S. Reed and G. Solomon, "Polynomial Codes Over Certain Finite Fields," *J. Soc. Ind. Appl. Math*, vol. 8, pp. 300-304, 1960.

[2] V. Guruswami and M. Sudan, "Improved Decoding of Reed-Solomon and algebraic-geometry codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1755-1764, September 1999.

[3] T. K. Moon, "Error Correction Coding: Mathematical Methods an Algorithms," 1st ed., Wiley, 2005.

[4] R. J. McEliece, "The Guruswami-Sudan Decoding Algorithm for Reed-Solomon Codes," *IPN Progress Report*, p.42-153, May 2003.

[5] R. Koetter and A. Vardy, "Algebraic soft-decision decoding of Reed-Solomon codes," *IEEE Trans. Inform. Theory*, vol. 49, no. 11, pp. 2809-2825, November 2003.

[6] F. Parvaresh, A. Vardy, "Multiplicity assignments for algebraic soft-decoding of Reed-Solomon codes," *Proc. Int. Symp. Inf. Theory*, July 2003, p.205.

[7] M. El-Khamy, R. J. McEliece, "Interpolation multiplicity assignment algorithms for algebraic soft-decision decoding of Reed-Solomon codes," *AMS-DIMACS.*, vol. 68, pp. 99-120, 2005. Vol. on Algebraic Coding Theory and Information Theory.

[8] N. Ratnakar, R. Koetter, "Exponential error bounds for algebraic soft-decision decoding of Reed-Solomon codes," *IEEE Trans. Inform. Theory*, vol. 51, p.3899-3917, Nov. 2005.

[9] J. Jiang, K. R. Narayanan, "Performance analysis of algebraic soft decoding of Reed-Solomon codes over binary symmetric and erasure channels," *Proc. ISIT*, Australia, Sep. 2005.

[10] E. R. Berlekamp, R. E. Peile, S. P. Pope, "The application of error control communications," *IEEE Commun. Mag.*, vol. 25, pp. 44-57, Jan. 1987.

[11] A. Vardy, Y. Be'ery, "Bit-level soft-decision decoding of Reed-Solomon codes," *IEEE Trans. Commun.*, vol. 39, pp. 440-445, Mar. 1991.

[12] W. J. Gross, F. R. Kschischang,R. Ktter, P. G. GulakR, "Applications of algebraic soft-decision decoding of Reed-Solomon codes ," *IEEE Trans. Commun.*, Jul., 2003.