Iterative Soft Decoding of Reed Solomon Codes

Jing Jiang, *Student Member, IEEE* and Krishna R. Narayanan, *Member, IEEE*
Department of Electrical Engineering, Texas A&M University, College Station, USA

***Abstract*— This letter presents an iterative decoding method for Reed Solomon (RS) codes. The proposed algorithm is a stochastic shifting based iterative decoding (SSID) algorithm which takes advantage of the cyclic structure of RS codes. The performances of different updating schemes are compared. Simulation results show that this method provides significant gain over hard decision decoding and is superior to some other popular soft decision methods for short RS codes.**

***Index Terms*— soft decision decoding, belief propagation, Reed Solomon codes.**

I. Introduction

BELIEF propagation (BP) based decoding has come to researchers' interest for its appealing performance in decoding sparse graph based codes, such as LDPC codes. High rate LDPC codes of short to medium lengths exhibit an undesirable error floor in high SNR region due to their small minimum distance. For this reason, several applications such as, for example, magnetic recording systems employ Reed Solomon (RS) codes, which possess good minimum distance. Consequently, soft decision decoding of RS codes is of practical value.

Currently popular soft decision decoding methods are Chase decoding [1], generalized minimum distance decoding, reliability based decoding [2] and more recently, the Koetter Vardy (KV) decoding algorithm [3] which is a soft-input algebraic decoding algorithm. An alternative approach is BP based iterative decoding. Iterative decoding of linear block codes and the sum product algorithm (SPA) was discussed in [4] [5]. It is commonly believed that BP algorithm is not suitable for high density parity check codes (HDPC), e.g., RS codes. Since the large number of short cycles in the factor graph will cause correlation between the messages and consequently incur "error propagation". Short block length codes with low density parity check matrices, which possess sparse Tanner graphs, were studied in [6]. However, these codes do not have as large minimum distance as RS codes do with comparable rate.

Recent research results of Yedidia $et\ al.$ [7] revealed the inherent connection between BP and statistical physics. However, the corresponding "generalized belief propagation (GBP)" algorithm they proposed [8] still has trouble in decoding HDPC codes over AWGN channel.

Nevertheless, their work on GBP inspired our study of BP algorithms for RS codes. In this paper, a stochastic shifting based iterative decoding (SSID) scheme is proposed to show that with proper scheduling, BP can perform well for RS codes.

II. Soft Decision Reed Solomon code Decoding

Consider a narrow sense RS code over $GF(q^m)$, $n = q^m - 1$, which has a minimum distance $\delta = n - k + 1$. With a bounded distance (BD) decoder, it is a $t = \lfloor(\delta - 1)/2\rfloor$ error correcting code. The parity check matrix can be represented by:

$$\mathbf{H} = \begin{pmatrix} 1 & \beta & \beta^2 & \dots & \beta^{(n-1)} \\ 1 & \beta^2 & \beta^4 & \dots & \beta^{2(n-1)} \\ & & & \dots & \\ 1 & \beta^{(\delta-1)} & \beta^{2(\delta-1)} & \dots & \beta^{(n-1)(\delta-1)} \end{pmatrix} \quad (1)$$

The matrix can also be expressed in a systematic or cyclic form. Here we consider RS codes over an extension field of $GF(2)$, i.e., $q = 2$. Let β be a primitive element in $GF(2^m)$, all the 2^m elements in $GF(2^m)$, 0, 1, β, β^2, $\cdots$, β^{2^m-2}, can be represented using a binary vector expansion in $GF(2)$. Summation operation in $GF(2^m)$ is nothing but the vector summation in $GF(2)$ and multiplication operation corresponds to binary matrix multiplication. Consequently, all the codewords and the parity check matrix can be represented in a binary vector form. Consider for example GF(4) and let β be a root of the primitive polynomial $p(x) = x^2 + x + 1$. β has the binary vector expansion $[0, 1]$ and the multiplication operation $\times\beta$ corresponds the binary multiplication of the vector expansion with a multiplication matrix: $\times\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, and etc.

By using this binary parity check matrix representation, RS decoding problem turns into a general problem of decoding of binary linear block codes [4]. Some research work has been focused on the construction of proper parity check sets for iterative decoding [5] [8], since the performance of iterative decoding will be different with the choice of parity check matrix even if the code is the same. Lucas $et\ al.$ [5] suggested using minimum weight parity check sets to propose iterative decoding. Some algorithms for the small weight parity check sets search is also referred. However, in general, finding a minimum parity check vector is NP-complete. In this work, it is shown that with proper scheduling, iterative decoding based on a "non-optimal" parity check matrix can still perform well.

III. Proposed Iterative Decoding Strategy

Suppose the coded bits are transmitted with BPSK modulation format (with 0 mapped to $+1$ and 1 mapped to -1) over AWGN channel,

$$\mathbf{y} = \mathbf{x} + \mathbf{n}, \quad (2)$$

Thus, the reliability of the received vector can be expressed in terms of their log-likelihood ratio (LLR) $\boldsymbol{L}(\mathbf{x})$ (here we use bold face letters to denote vectors). The *a posteriori* LLR of each bit can be expressed as:

$$\boldsymbol{L}(x_i) = \log \frac{P(c_i = 0|\mathbf{y})}{P(c_i = 1|\mathbf{y})}, \tag{3}$$

Though the exact *a posteriori* LLR of each bit is difficult to obtain, for sparse graph codes, a good approximation can be obtained using the BP algorithm. However, standard BP does not work well for HDPC codes due to "error propagation".

By taking advantage of the cyclic property of RS codes, a sum product algorithm (SPA) with a stochastic shifting schedule is proposed to help alleviate deterministic errors. Let $\boldsymbol{L}^{(j)}$ denote the sum of the received LLRs and all extrinsic LLR produced until the jth iteration. During the jth iteration, the SPA is used on the vector $\boldsymbol{L}^{(j)}$ to produce extrinsic information $\boldsymbol{L}_{ext}^{(j)}$. The LLR $\boldsymbol{L}^{(j+1)}$ is then updated according to:

$$\boldsymbol{L}^{(j+1)} = \boldsymbol{L}^{(j)} + \alpha \boldsymbol{L}_{ext}^{(j)}, \tag{4}$$

where $0 < \alpha \leq 1$ is a damping coefficient. The updated LLR $\boldsymbol{L}^{(j+1)}$ is cyclically shifted by θ symbols, where θ is a random integer unformly distributed between $(0, n-1)$. Since RS codes are cyclic, the cyclically shifted version of $\mathbf{x}$ is a valid codeword. Hence, a shifted version of $\boldsymbol{L}^{(j+1)}$ can be thought of as the received signal when a shifted version of another valid codeword was transmitted. Therefore, another iteration of the SPA is performed with the shifted version of the LLR $\boldsymbol{L}^{(j+1)}$. Since the geometry of the factor graph with the shifted version is different from the previous ones, deterministic errors can be suppressed. We continue this procedure for a predetermined number of times or until the parity checks are satisfied. When the maximum of j_{max} iterations is reached, another outer round, with a different realization of the random shifts and an increased α, begins with the original LLR from the channel, which prevents SPA decoding from getting stuck at pseudo-equilibrium points.

Define $\psi(\boldsymbol{L})$ as an one iteration of the SPA algorithm function with the input LLR $\boldsymbol{L}$. Define $\boldsymbol{L}_\theta$ as a cyclic shift of the vector by θ symbols (Note that received symbols should be shifted at symbol level). A detailed description of the algorithm is then given in Algorithm 1.

Kou *et al.* [9] also made use of the cyclic property of Geometry codes to construct redundant parity check matrix by cyclicly shifting parity check vectors, which is an exhaustive deterministic version of our method. Simulation results suggested that, the SSID based random updating scheme (RUS) outperforms the exhaustive parallel updating scheme (PUS). This is similar to the updating rules in a Hopfield network, where asynchronous and stochastic updating scheme outperforms synchronous updating scheme. The performance gain is believed to be mainly due to the stochastic shifting and multiple outer iteration rounds.

Algorithm 1 SSID algorithm for RS codes

```
Step1. Initialization: set $q = 0$, $j = 0$ and $\alpha_0$.
Step2. Set the coded bits LLR as observed from the channel:
       $\boldsymbol{L}^{(0)}(x_i) = \frac{2}{\sigma^2} y_i$.
Step3. SPA: Feed the LLRs into the decoder and generate
       extrinsic LLRs for each bit using SPA:
       $\boldsymbol{L}_{ext}^{(j)} = \psi(\boldsymbol{L}^{(j)})$.
Step4. Parameter Update: Update the LLR of each bit:
       $\boldsymbol{L}^{(j+1)}(x_i) = \boldsymbol{L}^{(j)}(x_i) + \alpha \boldsymbol{L}_{ext}^{(j)}(x_i)$.
       where $\alpha$ is a gradually increasing damping coefficient to control the updating step width.
Step5. Random Shifting: Cyclicly shift the LLRs by $\theta$
       symbols and record the overall shift $\Theta$:
       $\boldsymbol{L}^{(j+1)} \leftarrow \boldsymbol{L}_\theta^{(j+1)}$.
Step6. Hard Decision: $\hat{c}_i = \begin{cases} 0, & \boldsymbol{L}^{(j+1)}(x_i) > 0; \\ 1, & \boldsymbol{L}^{(j+1)}(x_i) < 0. \end{cases}$
Step7. Termination Criterion: If all the checks are satisfied,
       stop iteration and go to Step9, else if $j = j_{max}$, go
       to Step8, otherwise set $j \leftarrow j+1$ and go to Step3
       for another SPA iteration.
Step8. Outer Round: If $q = q_{max}$, declare a decoding
       failure, otherwise set $q \leftarrow q+1$ and $j = 0$, update the
       damping coefficient $\alpha = \alpha_0 + (q/(q_{max}-1))(1-\alpha_0)$
       and go to Step2 for another outer round.
Step9. Extract Information Bits: Shift the decoded bits back
       to their original position and get the information bits
       from coded bits. $\hat{\mathbf{c}} = \hat{\mathbf{c}}_{(-\Theta)}$
```

IV. Experimental Results and Discussion

In this section, simulation results for decoding of RS codes based on the SSID algorithm are presented. The initial damping coefficient α_0 is selected to be 0.08 based on simulation. Consider an RS(15,7) code and assume BPSK transmission over an AWGN channel. The performances of several updating schedules are shown in Fig. 1 along with the performance of the KV algorithm with a list size 4 taken from [10]. The updating schemes evaluated are: standard BP (300 iterations), RUS with a gradually changing damping coefficient (i.e., SSID), RUS with constant damping coefficient, serial updating scheme (SUS), PUS with redundant checks. Note that all the above schedules set a maximum 30 SPA iterations and 20 outer rounds and another RUS (with 30 SPA iterations and 300 outer rounds) is proposed of the same complexity with the PUS scheme, which uses redundant checks.

We note that standard BP outperforms hard decision decoding by 1.4 dB at an FER of 10^{-3}. However, further improvement can be achieved by proper updating and scheduling. RUS with gradually increasing damping coefficient outperforms that with constant damping coefficient, since it keeps updating damping coefficient from being either too conservative or too aggressive. RUS outperforms both PUS and SUS with the same complexity by 0.5 and 0.3 dB respectively. This is due to the fact that RUS can reduce deterministic error patterns and therefore improve the performance. The best result can be achieved so far is RUS with 300 outer rounds, which outperforms hard decision decoding by 3.1dB and the KV algorithm ($m_{max} = 4$) by about 2 dB at an FER of 10^{-5}.

An additional simulation of RS (15,7) is presented over fully interleaved Rayleigh fading channel (the decoding scheme is proposed with 300 outer rounds and 30 SPA iterations). Fig.

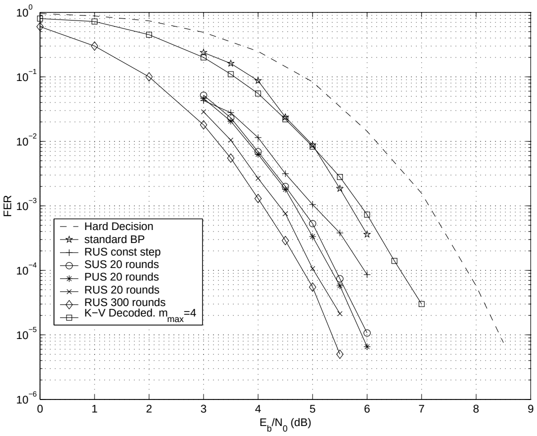

Fig. 1. RS (15,7) code with BPSK modulation over AWGN channel under different updating schemes.

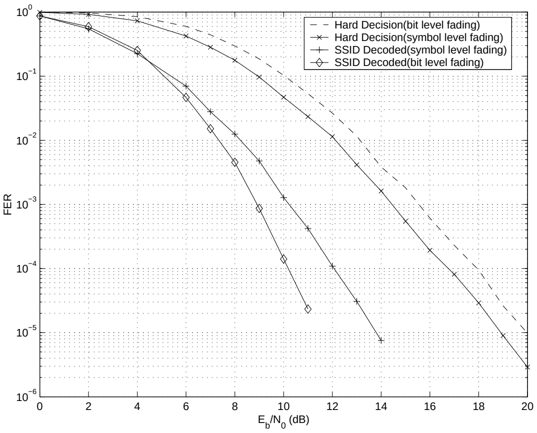

Fig. 2. RS (15,7) code with BPSK modulation over Rayleigh fading channel under SSID decoding.

2 suggests that the gain is even larger for fading channel, about 8.8dB for bit interleaving and about 5dB for symbol interleaving at an FER of 10^{-5}. This is mainly due to the performance degradation of BD decoding in a fading channel.

We present results for the RS (31,25) code over AWGN channel in Fig. 3. Several soft decision decoding methods are compared. For this code, standard BP algorithm has little gain due to the large number of short cycles. However, with SSID scheduling (with 200 outer rounds and 50 SPA iterations), the new method outperforms Berlekamp & Massey (BM) decoding, Generalized Minimum Distance (GMD) decoding and combined chase & GMD decoding, by 1.9dB, 1.3dB and 0.63dB, respectively at an FER of 10^{-4}. As mentioned previously, the performance gain is due to the beyond bounded sphere decoding capability of the proposed algorithm.

Unfortunately, we notice that the soft decision gain of the new method still diminishes as the codeword length becomes long (for a (63,55) code, which is not shown here, the gain is only 0.6dB compared with hard decision at an FER of 10^{-3}). However, the reason for performance loss under the BP algorithm is mainly due to the fact that the parity check matrix has high density and correlated unreliable information bits cause "error propagation". This is essentially different from other soft decision algorithms. We believe that more sophisticated decoding schemes can further improve the performance.

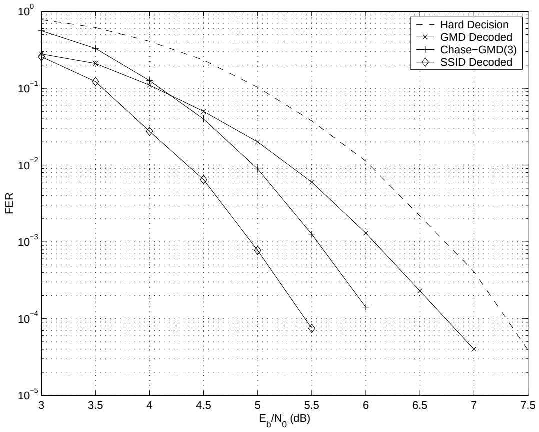

Fig. 3. RS (31,25) over AWGN channel under different decoding methods.

The worst case complexity of this scheme is quite high, i.e., the performance gain is obtained by running more outer rounds. However, the outer rounds and maximum iteration numbers are adjustable, which can offer reasonable trade-off between complexity and error correcting capability.

V. Conclusion

In this letter, a novel iterative soft decoding scheme for RS code has been proposed. We have shown that a properly scheduled BP algorithm outperforms algebraic decoding methods. This iterative decoding method can be readily extended to algebraic cyclic codes, such as BCH and Geometry codes. In principle, this decoding algorithm works for q^m-ary channels also, however the performance needs to be studied in more detail.

References

[1] N. Kamiya, "On algebraic soft-decision decoding algorithms for BCH codes", *IEEE Trans. Info Theory*, vol.47, pp.45-58, Jan. 2001

[2] M. Fossorier, S. Lin, "Soft Decision Decoding of Linear Block Codes Based on Ordered Statistics", *IEEE Tran. Info Theory*, pp.1379-1396, Sept. 1995.

[3] R. Koetter, A. Vardy, "Algebraic Soft-Decision Decoding of Reed-Solomon Codes", *IEEE Trans. Info Theory*, submitted 2001.

[4] J. Hagenauer, E. Offer, L. Papke, "Iterative decoding of binary block and convolutional codes", *IEEE Trans. Info Theory*, vol.42, pp. 429-445, Mar. 1996

[5] R.Lucas, M. Bossert, M. Breitbach, "On iterative soft-decision decoding of linear binary block codes and product codes", *IEEE Journal Selected Areas in Communications*, vol.16, pp. 276-296, Feb. 1998

[6] Y. Kou, S. Lin, M. P. C. Fossorier, "Low-density parity-check codes based on finite geometries: a rediscovery and new results", *IEEE Trans. Info Theory*, vol.47, pp. 2711-2736, Nov. 2001

[7] J. S. Yedidia, W. T. Freeman, Y. Weiss, "Constructing Free Energy Approximations and Generalized Belief Propagation Algorithms", *Merl Technical Report: TR2002-35*, Oct. 2002, available online at http://www.merl.com/papers/TR2002-35/

[8] J. S. Yedidia, J. Chen, M. Fossorier, "Generating Code Representations Suitable for Belief Propagation Decoding", *Proc. Allerton'2002*, Illinois Oct. 2002

[9] Y. Kou, J. Xu, H. Tang, S. Lin, K. Abdel-Ghaffar, "On circulant low density parity check codes", *Proc. ISIT'2002*, pp.200 Lausanne Jun. 2002

[10] W.J. Gross, F.R. Kschischang, R. Koetter, P.G. Gulak, "Simulation Results for Algebraic Soft-Decision Decoding of Reed-Solomon Codes", Proc. of 21st Biennial Symp. on Comm, pp. 356-360, Kingston, CA. Jun. 2002