Bit-Level Soft-Decision Decoding of Triple-Parity Reed-Solomon Codes through Automorphism Groups

Vo Tam Van, Seiichi Mita, Jing (Tiffany) Li, Chau Yuen, and Yong Liang Guan

Abstract—This paper discusses bit-level soft decoding of triple-parity Reed-Solomon (RS) codes through automorphism permutation. A new method for identifying the automorphism groups of RS binary images is first developed. The new algorithm runs effectively, and can handle more RS codes and capture more automorphism groups than the existing ones. Utilizing the automorphism results, a new bit-level soft-decision decoding algorithm is subsequently developed for general $(n, n-3, 4)$ RS codes. Simulation on $(31, 28, 4)$ RS codes demonstrates an impressive gain of more than 1 dB at the bit error rate of 10^{-5} over the existing algorithms.

Index Terms—Reed Solomon codes, automorphism groups, permutation decoding, binary images, soft decoding.

I. INTRODUCTION

REED-SOLOMON (RS) codes, with their renowned Berlekamp-Massey and Forney algorithms, boast robust error correcting capability against bit-flip errors such as large amplitude fluctuation errors and burst errors. However, to fully harness their power on additive white Gaussian noise (AWGN) channels requires effective soft decoding, which has been a research focus in recent years (see, for example, [2], [8]).

Some algorithms, such as sorting- and scheduling- based message-passing algorithms, are designed for general RS codes [2], [8]. Not restricting the underlying code specifications, these algorithms achieve generality at the cost of a rather high level of computational complexity. In comparison, the algorithms that target specific classes of RS codes can explore specific code structures to effectively reduce the complexity and/or improve the performance. Among the latter type, a notable example is the bit-level automorphism-based decoder developed in [3], which is designed for double-parity RS codes. Working especially well for short-length (double-parity) RS codes, the algorithm in [3] is shown to be capable of a performance within 0.3dB to the maximum likelihood decoder (MLD) at a bit error rate (BER) of 10^{-5}. Despite its efficiency, however, this algorithm cannot handle RS codes of more than two parity symbols, in part due to its incapability of obtaining their automorphism groups.

This paper studies bit-level soft decoding of triple-parity RS codes. Motivated by the algorithm in [3], we first investigate the automorphism groups of the binary images of a general

$(n, n-3, 4)$ RS code, and propose a heuristic search permutation algorithm to identify the automorphism groups. Through concrete examples, we show that our algorithm works effectively, can handle codes that previous algorithms cannot, and find automorphism groups that previous algorithms cannot. Exploiting these automorphism groups and integrating them with the general-purpose soft decoder (rather than the hard decoder in [3]), we further develop a new bit-level soft decoding algorithm, termed *permutation sum-product algorithm* (PSPA), for triple-parity RS codes. Simulation demonstrates that our algorithm can noticeably outperform the existing algorithms, such as conventional hard-decision decoding (HDD) [1] and the soft-decision SPA [6]. The proposed new algorithm is most efficient for short-length RS codes, and can be extended to soft decode concatenated or compound codes that use short-length triple-parity RS codes as the component code.

The rest of the paper is organized as follows. Section II introduces the binary image of RS codes. Section III discusses automorphism groups and details our searching algorithms for $(n, n-3, 4)$ RS binary images. Section IV presents a new soft decoding method that effectively combines automorphism permutations and soft-decision sum product algorithm (SPA). Section V demonstrates simulation results, and Section VI concludes the paper.

II. BINARY IMAGES OF RS CODES

Let $\gamma = [\gamma_1, \gamma_2, \cdots, \gamma_m]$ be a basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. Let the code length be $n = 2^m - 1$. The binary image of a double-parity $(n, n-2, 3)$ RS codeword $\mathbf{c} = [c_0, c_1, \cdots, c_{n-1}]$ is an $m \times n$ binary matrix:

$$B_M(\mathbf{c}) := \begin{bmatrix} c_{1,0} & c_{1,1} & c_{1,2} & \cdots & c_{1,n-1} \\ c_{2,0} & c_{2,1} & c_{2,2} & \cdots & c_{2,n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ c_{m,0} & c_{m,1} & c_{m,2} & \cdots & c_{m,n-1} \end{bmatrix}, \quad (1)$$

where $c_j = c_{1,j}\gamma_1 + c_{2,j}\gamma_2 + \cdots + c_{m,j}\gamma_m$ and $c^{(i)} = [c_{i,0}, c_{i,1}, c_{i,2}, \cdots, c_{i,n-1}]$ for all $j \in \mathbb{Z}_n$ and $1 \le i \le m$.

The parity check matrix of the $(n, n-2, 3)$ RS binary image with zeros $\{1, \alpha\}$ can be presented by a $2m \times m$ polynomial in the ring $\mathbb{F}_2[x]/(x^n - 1)$ [3]:

$$\begin{bmatrix} \theta_1(x) & 0 & \cdots & 0 \\ 0 & \theta_1(x) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \theta_1(x) \\ \theta_\varepsilon(x)x^{u_1} & \theta_\varepsilon(x)x^{u_2} & \cdots & \theta_\varepsilon(x)x^{u_m} \\ \vdots & \vdots & \vdots & \vdots \\ \theta_\varepsilon(x)x^{u_1+m-1} & \theta_\varepsilon(x)x^{u_2+m-1} & \cdots & \theta_\varepsilon(x)x^{u_m+m-1} \end{bmatrix},$$

$$(2)$$

TABLE I
u VECTORS COMPUTED FOR $\gamma = [\gamma_1, \gamma_2, \cdots, \gamma_m]$.

	Vector **u**	Primitive element α
$\mathbb{F}_{2^3}$	$[2, 1, 0]^T$	$\alpha^3 = \alpha + 1$
$\mathbb{F}_{2^4}$	$[2, 1, 0, 14]^T$	$\alpha^4 = \alpha + 1$
$\mathbb{F}_{2^5}$	$[30, 29, 28, 27, 26]^T$	$\alpha^5 = \alpha^2 + 1$
$\mathbb{F}_{2^6}$	$[4, 3, 2, 1, 0, 62]^T$	$\alpha^6 = \alpha + 1$

TABLE II
COMMON VECTORS $\mathbf{u}^{(1)}$ AND $\mathbf{u}^{(2)}$ FOR $(n, n-3, 4)$ RS CODES.

	Vector $\mathbf{u}^{(1)}$	Vector $\mathbf{u}^{(2)}$
$\mathbb{F}_{2^3}$	$[2, 1, 0]^T$	$[2, 5, 1]^T$
$\mathbb{F}_{2^4}$	$[2, 1, 0, 14]^T$	$[2, 9, 1, 8]^T$
$\mathbb{F}_{2^5}$	$[30, 29, 28, 27, 26]^T$	$[30, 14, 29, 13, 28]^T$
$\mathbb{F}_{2^6}$	$[4, 3, 2, 1, 0, 62]^T$	$[4, 35, 3, 34, 2, 33]^T$
$\mathbb{F}_{2^7}$	$[6, 5, 4, 3, 2, 1, 0]^T$	$[6, 69, 5, 68, 4, 67, 3]^T$
$\mathbb{F}_{2^8}$	$[4, 3, 2, 1, 0, 254, 253, 252]^T$	$[4, 131, 3, 130, 2, 129, 1, 128]^T$
$\mathbb{F}_{2^9}$	$[510, 509, 508, 507, 506,$ $505, 504, 503, 502]^T$	$[510, 254, 509, 253, 508,$ $252, 507, 251, 506]^T$
$\mathbb{F}_{2^{10}}$	$[6, 5, 4, 3, 2, 1, 0,$ $1022, 1021, 1020]^T$	$[6, 517, 5, 516, 4, 515,$ $3, 514, 2, 513]^T$

where $\varepsilon = \alpha^{-1}$, $\theta_\varepsilon(x)$ is known as the *idempotent* [4], and $\theta_1(x) = 1 + x + x^2 + \cdots + x^{n-1}$. Examples of vectors $\mathbf{u} = (u_1, u_2, \cdots, u_m) \in \mathbb{Z}_n^m$ are listed in Table I.

III. AUTOMORPHISMS OF TRIPLE-PARITY RS CODES

Previous work has reported all the automorphism groups for the $(7, 4, 4)$ RS code over $\mathbb{F}_{2^3}$ and part of the automorphism groups for the $(15, 12, 4)$ RS code over $\mathbb{F}_{2^4}$ [3]. Here, we focus on general $(n, n-3, 4)$ RS codes with zeros $\{1, \alpha, \alpha^2\}$ over $\mathbb{F}_{2^m}$ for all $m \geq 4$. Since, α and α^2 belong to the same cyclotomic coset, the parity check matrix of $(n, n-3, 4)$ RS codes is represented by the following $3m \times m$ polynomial matrix in the ring $\mathbb{F}_2[x]/(x^n - 1)$.

$$
\begin{bmatrix}
\theta_1(x) & 0 & \cdots & 0 \\
0 & \theta_1(x) & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots \\
0 & 0 & \cdots & \theta_1(x) \\
\theta(x)x^{u_1^{(1)}} & \theta(x)x^{u_2^{(1)}} & \cdots & \theta(x)x^{u_m^{(1)}} \\
\vdots & \vdots & \vdots & \vdots \\
\theta(x)x^{u_1^{(1)}+m-1} & \theta(x)x^{u_2^{(1)}+m-1} & \cdots & \theta(x)x^{u_m^{(1)}+m-1} \\
\theta(x)x^{u_1^{(2)}} & \theta(x)x^{u_2^{(2)}} & \cdots & \theta(x)x^{u_m^{(2)}} \\
\vdots & \vdots & \vdots & \vdots \\
\theta(x)x^{u_1^{(2)}+m-1} & \theta(x)x^{u_2^{(2)}+m-1} & \cdots & \theta(x)x^{u_m^{(2)}+m-1}
\end{bmatrix},
\tag{3}
$$

where $\theta(x)$ is short for $\theta_\varepsilon(x)$. The vectors $\mathbf{u}^{(1)} = [u_1^{(1)}, u_2^{(1)}, \cdots, u_m^{(1)}]$ and $\mathbf{u}^{(2)} = [u_1^{(2)}, u_2^{(2)}, \cdots, u_m^{(2)}] \in \mathbb{F}_n^m$ can be computed using the method introduced in [3], and the results are listed in Table II.

Define the symmetric group on the set $\{1, 2, \cdots, m\}$ as Ω_m. A permutation $\sigma \in \Omega_m$ is represented using the cycle notation (e.g., the permutation $\sigma = (1, 2, 4)$ means $\sigma(1) = 2$, $\sigma(2) = 4$, and $\sigma(4) = 1$). Let id denote the identity permutation on m indices $\{1, 2, \cdots, m\}$. Let $a_1, a_2, \cdots, a_m \in \mathbb{Z}_n$ and $l \in \mathbb{Z}_m$. The parameter $(\sigma, (a_1, a_2, \cdots, a_m), l)$ completely describes the permutation ρ, such that $[i, j] \mapsto [\sigma(i), j2^l + a_i]$.

We present the basic idea of identifying the automorphism through the following example.

Example 1: [$(15, 12, 4)$ RS code] Let α be a fixed primitive element satisfying $\alpha^4 = \alpha + 1$. Consider the $(15, 12, 4)$ RS binary image with zeros $\{1, \alpha, \alpha^2\}$, imaged under the canonical basis.

Consider a specific permutation ρ that is described by the parameters $\sigma = (1, 2)(3, 4)$, (a_1, a_2, a_3, a_4) and l. It can be verified that the permutations $(\sigma, (a_1, a_2, \cdots, a_m), l)$ and $(\sigma, (a_1, a_2, \cdots, a_m) + a, l)$ belong to the same automorphism group. Therefore, it is sufficient to fix parameter $a_1 = 0$, then ρ maps the indices

$$
\begin{array}{ll}
[1, j] \mapsto [2, j2^l], & [2, j] \mapsto [1, j2^l + a_2] \\
[3, j] \mapsto [4, j2^l + a_3], & [4, j] \mapsto [3, j2^l + a_4]
\end{array}
\tag{4}
$$

The parity check matrix of the $(15, 12, 4)$ RS binary image is invariant under the permutation specified in (4), if and only if the following generator matrix in the ring $\mathbb{F}_2[x]/(x^{15} - 1)$ is invariant under permutation specified in (4):

$$
\begin{bmatrix}
0 & \theta(x)x^{b_{12}} & \theta(x)x^{b_{13}} & \theta(x)x^{b_{14}} \\
\theta(x)x^{b_{21}} & 0 & \theta(x)x^{b_{23}} & \theta(x)x^{b_{24}} \\
\theta(x)x^{b_{31}} & \theta(x)x^{b_{32}} & 0 & \theta(x)x^{b_{34}} \\
\theta(x)x^{b_{41}} & \theta(x)x^{b_{42}} & \theta(x)x^{b_{43}} & 0
\end{bmatrix},
\tag{5}
$$

where $(b_{12}, b_{13}, b_{14}) = (7, 12, 1)$, $(b_{21}, b_{23}, b_{24}) = (8, 14, 4)$, $(b_{31}, b_{32}, b_{34}) = (14, 0, 6)$, and $(b_{41}, b_{42}, b_{43}) = (4, 6, 7)$.

Note that permuting $\theta(x)x^r$ by $j \mapsto 2^l j$ is equivalent to $(\theta(x)x^r)^{2^l} = \theta(x)x^{r2^l}$, since $\theta(x)$ is an idempotent and $\theta(x)^2 = \theta(x)$. Consider $[0, \theta(x)x^{b_{12}}, \theta(x)x^{b_{13}}, \theta(x)x^{b_{14}}]$ from the $\mathbb{F}_2$-rowspace of (5). Applying the permutation (4), this row permutes to
$[0, \theta(x)x^{b_{12}}, \theta(x)x^{b_{13}}, \theta(x)x^{b_{14}}] \rightarrow$
$\qquad [\theta(x)x^{2^l b_{12}+a_2}, 0, \theta(x)x^{2^l b_{14}+a_4}, \theta(x)x^{2^l b_{13}+a_3}]$.
Permutation ρ belong to the code automorphism group if the following two vector $[\theta(x)x^{2^l b_{12}+a_2}, 0, \theta(x)x^{2^l b_{14}+a_4}, \theta(x)x^{2^l b_{13}+a_3}]$ and $[\theta(x)x^{b_{21}}, 0, \theta(x)x^{b_{23}}, \theta(x)x^{b_{24}}]$ are generated from the same basis vector. This leads to the following equation

$$
\begin{cases}
\Delta_1 = \mod(2^l b_{12} + a_2 - b_{\sigma(1),\sigma(2)}, n) \\
\Delta_2 = \mod(2^l b_{13} + a_3 - b_{\sigma(1),\sigma(3)}, n) \\
\Delta_3 = \mod(2^l b_{14} + a_4 - b_{\sigma(1),\sigma(4)}, n) \\
\quad \Delta_1 = \Delta_2 = \Delta_3
\end{cases}
\tag{6}
$$

Let $\Delta_1 = \Delta_2 = \Delta$, then $a_i = \mod(\Delta + b_{\sigma(1),\sigma(i)} - 2^l b_{1i}, n)$. It can be seen that when $l = 0$, we obtain $(a_2, a_3, a_4) = (12, 3, 9)$. To verify ρ belong to the code automorphism group, we consider $[\theta(x)x^{8+r}, 0, \theta(x)x^{14+r}, \theta(x)x^{4+r}]$ from the $\mathbb{F}_2$-rowspace of (5). The permutation (4) gives rise to
$[\theta(x)x^{8+r}, 0, \theta(x)x^{14+r}, \theta(x)x^{4+r}] \rightarrow$
$\qquad [0, \theta(x)x^{8+r}, \theta(x)x^{13+r}, \theta(x)x^{2+r}]$
which again lies in the $\mathbb{F}_2$-rowspace of (5). Thus, ρ belongs to the automorphism group of the $(15, 12, 4)$ RS binary images generated by the matrix in (3). $\qquad \square$

To find the other permutations of a general $(n, n-3, 4)$ RS code, we propose an effective search permutation algorithm, which is the generalization of the above example. Note that

TABLE III
AUTOMORPHISMS OF $(15, 12, 4)$ RS CODE WITH ZEROS $\{1, \alpha, \alpha^2\}$.

σ	(a_1, a_2, a_3, a_4)	l
id	$(0, 0, 0, 0) + a$	0
$(1, 2)(3, 4)$	$(0, 12, 3, 9) + a$	0
$(1, 3)(2, 4)$	$(0, 3, 6, 3) + a$	0
$(1, 4)(2, 3)$	$(0, 9, 3, 12) + a$	0
$(2, 4)$	$(0, 3, 9, 3) + a$	2
$(4, 3, 2, 1)$	$(0, 0, 12, 12) + a$	2
$(1, 3)$	$(0, 6, 0, 6) + a$	2
$(1, 2, 3, 4)$	$(0, 12, 12, 0) + a$	2

there exists a set of constants $\{b_{i,j} : 1 \leq i, j \leq m, \ i \neq j\}$ in $\mathbb{Z}_n$, whereby the rows of the following $m \times m$ matrix $\mathbf{M}$:

$$\mathbf{M} := \begin{bmatrix} 0 & \theta(x)x^{b_{12}} & \cdots & \theta(x)x^{b_{1m}} \\ \theta(x)x^{b_{21}} & 0 & \cdots & \theta(x)x^{b_{2m}} \\ \vdots & \vdots & \ddots & \vdots \\ \theta(x)x^{b_{m,1}} & \cdots & \theta(x)x^{b_{m,m-1}} & 0 \end{bmatrix} \tag{7}$$

lie in the $\mathbb{F}_2$-rowspace of (3). Specifically, (5) in the previous subsection is but a particular case of (7) with $m = 4$ and was reported in [3]. The proposed search algorithm is described below and has a complexity $O(m!n^2m)$.

Heuristic permutation search algorithm

Input: Polynomial matrix $\mathbf{M}$ in (7).

Output: The automorphism group $\mathbf{P}$.

1. **forall** $\sigma \in \Omega_m$, $a_2, a_3 \in \mathbb{Z}_n$ and $l \in \mathbb{Z}_m$

2. Compute $\begin{cases} \Delta_1 = \mod(2^l b_{12} + a_2 - b_{\sigma(1),\sigma(2)}, \ n) \\ \Delta_2 = \mod(2^l b_{13} + a_3 - b_{\sigma(1),\sigma(3)}, \ n) \end{cases}$

3. If $\Delta_1 = \Delta_2$, then $a_i = \mod(\Delta_1 + b_{\sigma(1),\sigma(i)} - 2^l b_{1i}, \ n)$ where $3 \leq i \leq m$; otherwise **continue**.

4. Construct a permutation $\rho = (\sigma, (0, a_2, \cdots, a_m), l)$.

5. If $\mathbf{M}$ is invariant under ρ, then store ρ in $\mathbf{P}$.

6. **end**

Example 1 cont'd: [$(15, 12, 4)$ **RS code**] Table III presents all the permutations of the $(15, 12, 4)$ RS binary images with zeros $\{1, \alpha, \alpha^2\}$, obtained by the proposed algorithm. We report a total of 120 unique code automorphisms, 15 of which map $[i, j] \mapsto [i, j + a]$ for all $a \in \mathbb{Z}_{15}$. In general, it appears that the permutation $\rho = (\sigma, (a_1, a_2, \cdots, a_m), 0)$, where $\sigma = (1, n)(2, n - 1) \cdots$ and $(a_1, a_2, \cdots, a_m) = (0, (2^{m-1} + 1), 3, (2^{m-1} + 1) + 3, 6, (2^{m-1} + 1) + 6, \cdots) + a$ belongs to the automorphism group of the $(n, n - 3, 4)$ RS binary images for all m and $a \in \mathbb{Z}_n$. $\square$

Example 2: [$(31, 28, 4)$ **RS code**] Consider the $(31, 28, 4)$ RS binary image with zeros $\{1, \alpha, \alpha^2\}$, where α is a fixed primitive element satisfying $\alpha^5 = \alpha^2 + 1$, imaged under the canonical basis. The parity check matrix of this binary image is invariant under permutation ρ, if and only if the following polynomial matrix in the ring $\mathbb{F}_2[x]/(x^{31} - 1)$ is invariant under permutation ρ:

$$\begin{bmatrix} 0 & \theta(x)x^6 & \theta(x)x^{12} & \theta(x)x^{15} & \theta(x)x^{24} \\ \theta(x)x^{22} & 0 & \theta(x)x^5 & \theta(x)x^{11} & \theta(x)x^{14} \\ \theta(x)x^{14} & \theta(x)x^{22} & 0 & \theta(x)x^5 & \theta(x)x^{11} \\ \theta(x)x & \theta(x)x^{12} & \theta(x)x^{20} & 0 & \theta(x)x^3 \\ \theta(x)x^{28} & \theta(x)x^2 & \theta(x)x^{13} & \theta(x)x^{21} & 0 \end{bmatrix} \tag{8}$$

Applying the proposed search algorithm leads to Table IV.

TABLE IV
AUTOMORPHISMS OF $(31, 28, 4)$ RS CODE WITH ZEROS $\{1, \alpha, \alpha^2\}$.

σ	$(a_1, a_2, a_3, a_4, a_5)$	l
id	$(0, 0, 0, 0, 0) + a$	0
$(1, 2)(4, 5)$	$(0, 15, 23, 29, 17) + a$	0
$(1, 4)(2, 5)$	$(0, 29, 9, 18, 20) + a$	0
$(1, 5)(2, 4)$	$(0, 17, 3, 20, 6) + a$	0

TABLE V
AUTOMORPHISM SUBGROUP ORDERS OF $(n, n - 3, 4)$ RS CODES OVER FINITE FIELD $\mathbb{F}_{2^m}$ OBTAINED BY THE PROPOSED SEARCH ALGORITHM. (N.A. MEANS NOT AVAILABLE)

	Proposed	MAGMA [5]	Lim *et al.* [3]
$\mathbb{F}_{2^4}$	120	120	18
$\mathbb{F}_{2^5}$	124	124	N.A
$\mathbb{F}_{2^6}$	126	126	N.A
$\mathbb{F}_{2^7}$	254	254	N.A
$\mathbb{F}_{2^8}$	510	N.A	N.A

We identify a total of 124 unique code automorphisms, 31 of which map $[i, j] \mapsto [i, j + a]$ for all $a \in \mathbb{Z}_{31}$. $\square$

Example 3: [General $(n, n - 3, 4)$ **RS codes]** The number of all the automorphism groups found via the proposed algorithm is listed in Table V, for several $(n, n - 3, 4)$ RS codes. We also present the code automorphism orders computed using MAGMA software. Compared to the existing algorithms, our algorithm finds significantly more automorphisms than the method in [3]; It produces results consistent with those obtained from the MAGMA computation in [5][1], but can handle fields of larger orders (e.g. $\mathbb{F}_{2^8}$) where MAGMA would face difficulty. $\square$

IV. SOFT DECODING OF $(n, n - 3, 4)$ RS CODES

The availability of a list of the permutation groups allows us to develop more effective soft decoders for triple-parity RS codes. The proposed new *permutation sum-product algorithm*, illustrated in Fig. 1, takes advantage of the rich permutation groups obtained in Section III and the soft decision output of the classical (binary) sum-product algorithm.

Permutation sum-product algorithm (PSPA)

Input: Observation $\mathbf{y}$

Output: corrected codeword.

1. Represent $\mathbf{y}$ as a binary image. Decode $\mathbf{y}$ using the conventional sum-product algorithm (SPA).

2. If the SPA produces a valid codeword $\mathbf{c}$, then stop; otherwise store the log-likelihood $\hat{\mathbf{y}}$

3. Generate a random permutation $\mathbf{y}$: $\mathbf{y}_\rho = \rho(\mathbf{y})$ (e.g. using the proposed search algorithm).

4. Repeat step 1 until all the permutations are exhausted or a maximum number of trials is reached.

5. Compute the sum: $\mathbf{y}_{sum} = \hat{\mathbf{y}} + \sum \rho^{-1}(\hat{\mathbf{y}}_\rho)$.

6. Perform hard decision on $\mathbf{y}_{sum}$ and outputs the result.

Remark: It should be noted that our decoding algorithm differs from that proposed in [7]. The algorithm in [7] is restricted to binary cyclic codes over binary erasure channels. Our problem here involves the general permutations of bit-level RS codes over AWGN channels, and the cyclic codes in [7] may be viewed as a special case of ours. Our decoder also

---

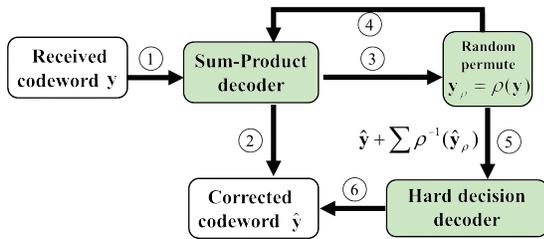[1] Note that two groups of the same order do not imply the same.

Fig. 1. Permutation sum-product algorithm for $(n, n-3, 4)$ RS binary images.

Fig. 2. BER performance for $(31, 28, 4)$ RS code over AWGN channels.

Fig. 3. BER performance for $(63, 60, 4)$ RS code over AWGN channels.

differs from that in [3]. To achieve its desirable performance, the decoder in [3] must be able to find a "perfect" permutation that gathers all of the bit errors in one symbol, and then decode this permutation using some *hard-decision* decoder. Not only is such a perfect permutation very difficult to identify, but the decoder performance would also degrade very quickly should a perfect permutation become unavailable. In comparison, our PSPA method obviates the burden of identifying a perfect permutation, simply takes in random permutations, and exploits the power of the *soft-decision* SPA to effectively correct bit errors.

V. Simulation results

Simulations are conducted to verify the effectiveness of the proposed decoding algorithm. The triple-parity $(31, 28, 4)$ and $(63, 60, 4)$ RS codes over $\mathbb{F}_{2^5}$ and $\mathbb{F}_{2^6}$ are considered. We compare our proposed soft-decision PSPA algorithm with three other systems: the uncoded system, the RS code with the conventional hard-decision decoding (HDD) implementing the Berlekamp-Massey algorithm [1], and the RS code with the soft-decision sum-product algorithm (SPA) [6]. Since the decoder in [3] only work for double-parity RS codes, it is not included in the comparison.

In the proposed PSPA, the maximum number of decoding iteration is set to 30 for the embedded sum-product decoder, and the number of random permutations (trials) is set to 10 (i.e. at the most 10 automorphism permutations are chosen randomly from the 4 classes in Table IV). As shown in Fig. 2 and Fig. 3, our PSPA noticeably outperforms the hard-decision decoder and the soft-decision SPA by more than 1 dB at a BER of 10^{-5}. This impressive performance gain is attainable because automorphism permutations lead to new and different decoding matrices, opening the possibility to break up some critical short cycles or trapping sets that were previously preventing the SPA algorithm from converging.

VI. Conclusion

We have investigated the bit-level soft decoding of triple-parity $(n, n-3, 4)$ RS codes. We first proposed an effective search algorithm to identify automorphism groups of a general $(n, n-3, 4)$ RS code with zeros $\{1, \alpha, \alpha^2\}$, and next developed a soft-decoding algorithm that integrates automorphism permutation and the conventional soft-decision sum product algorithm. Simulations confirm the effectiveness of the proposed *permutation sum-product algorithm*, revealing an impressive performance of more than 1 dB at the BER of 10^{-5} than the existing algorithms. Our algorithm is particularly suitable for short-length triple-parity RS codes, or concatenated codes in which they are a component code.
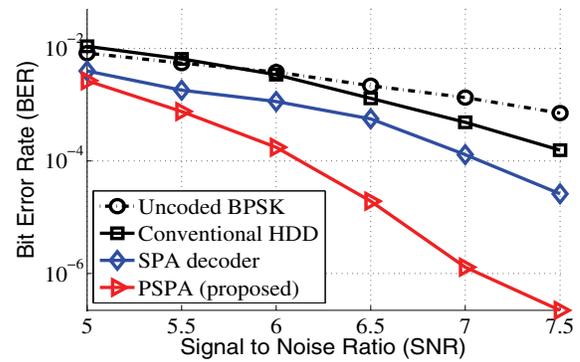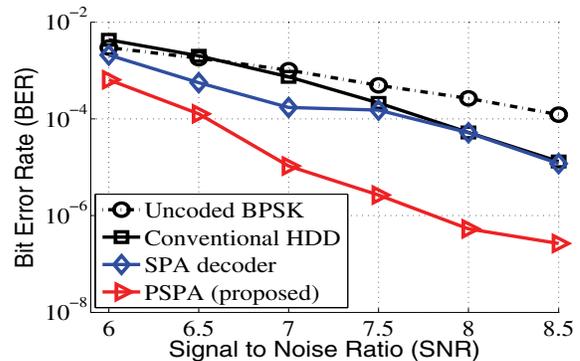
References

[1] E. R. Berlekamp, *Algebraic Coding Theory*. McGraw-Hill, 1968.
[2] J. Jiang *et al.*, "Algebraic soft-decision decoding of RS codes using bit-level soft information," *IEEE Trans. Inf. Theory,* vol. 54, no. 9, 2008.
[3] F. Lim *et al.*, "Code automorphisms and permutation decoding of certain RS binary images," *IEEE Trans. Inf. Theory,* vol. 56, no. 10, 2010.
[4] F. J. MacWilliams *et al.*, *The Theory of Error Correcting Codes*, 2nd edition. North-Holland, 1983.
[5] W. Bosma *et al.*, "The Magma algebra system—I: the user language," *J. Symbolic Comput.*, vol. 24, pp. 235–265, 1997.
[6] J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. Morgan Kaufmann, 1988
[7] T. Hehn *et al.*, "Permutation decoding and the stopping redundancy hierarchy of cyclic and extended cyclic codes," *IEEE Trans. Inf. Theory* vol. 54, no. 12, 2008.
[8] A. Vardy *et al.*, "Bit level soft-decision decoding of Reed-Solomon codes," *IEEE Trans. Inf. Theory* vol. 39, no. 3, pp. 440–444, 1991.