Curve-Fitting Based Decoding of GII-RS Codes

Xinzheng He[†‡], Li Chen[†‡] and Yingquan Wu[§]
[†] School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou, China
[‡] Guangdong Provincial Key Laboratory of Information Security Technology, Guangzhou, China
[§] MBZUAI Institute of Foundation Models, CA, USA
Email: hexzh9@mail2.sysu.edu.cn, chenli55@mail.sysu.edu.cn, yingquan_wu@yahoo.com

2026 IEEE International Symposium on Information Theory (ISIT) | 979-8-3315-8004-9/26/$31.00 ©2026 IEEE | DOI: 10.1109/ISIT62367.2026.11653801

***Abstract*—Generalized integrated interleaved (GII) codes can achieve an enhanced error-correction capability for an array of interleaves which are also known as component codes. With Reed-Solomon (RS) component codes, the GII codes are called GII-RS codes. So far, only syndrome-based decoding has been developed for GII-RS codes, leaving their error-correction potential unfully exploited. Curve-fitting based decoding, i.e., the Guruswami-Sudan (GS) algorithm, possesses improved error-correction capability. This paper first generalizes the decoding of GII codes into determining the error patterns for the corrupted interleaves. Subsequently, the curve-fitting based decoding is proposed for GII-RS codes. The soft-decision decoding is further proposed for GII-RS codes, in which the celebrated Kötter-Vardy (KV) algorithm is employed. Their improved error-correction performance is demonstrated numerically.**

***Index Terms*—Encoding and decoding, generalized integrated interleaved (GII) codes, linear block codes, RS codes**

I. Introduction

Future data communication systems lay new demands for channel coding techniques, which shall encompass not only a high decoding performance but also a high throughput. Generalized integrated interleaved (GII) codes [1] are one of the promising candidates that can meet both demands. A $([\rho, v], n)$ GII code consists of ρ interleaves of length n. Linear combinations of the interleaves can generate v nested codewords with stronger error-correction capabilities. Decoding of the ρ interleaves can be performed in parallel. If there remain interleaves undecoded, the nested codes can be incurred for enhancing error-correction capability of the remaining interleaves, leading to both high decoding throughput and performance. So far, only Reed-Solomon (RS) codes and BCH codes have been considered as interleaves in the GII paradigm, where the decoding is limited to the conventional syndrome-based approach, i.e., the Berlekamp-Massey (BM) algorithm [2]. Encoding and decoding of GII-RS codes and GII-BCH codes were improved in [3]–[9]. Meanwhile, theoretical analysis of hard-decision decoding performance for GII-BCH codes was first studied in [1] and later improved in [10].

Under the GII paradigm, we call all the interleaves the front layer codes. Subsequently, the nested codes are called the first layer code, the second layer code, and etc. They are ordered through decreasing dimensions. Linear combination of the front layer codewords yields a nested layer codeword. GII codes improve error-correction capability of the interleaves through exploiting such a nested codebooks property. For the existing syndrome-based decoding, this property enables higher order syndromes to be computed, correcting more error patterns that were not able to be handled by only the front layer codes. The curve-fitting based decoding, i.e., the Guruswami-Sudan (GS) algorithm [11], possesses an improved error-correction capability over the syndrome-based decoding, allowing the number of correctable errors to exceed half of the code's minimum Hamming distance. Meanwhile, limited by knowledge on the decoding of GII codes, there only exists Chase decoding [12] as the soft-decision decoding for GII codes.

This paper generalizes the decoding of GII-RS codes and further proposes the performance enhancing curve-fitting based decoding for the codes. Our generalization shows decoding of a GII code can be seen as finding error patterns for its corrupted interleaves. Hence, the curve-fitting based decoding is proposed for the GII-RS codes, where the GS algorithm is applied to decode the interleaves and the nested codewords. Since the nested codes are of lower dimensions, the GS algorithm becomes more favorable in error-correction. Subsequently, the more efficient soft-decision decoding, in which the celebrated Kötter-Vardy (KV) [13] algorithm is employed, is further proposed for GII-RS codes. As a result, decoding performance of GII-RS codes can be substantially improved over the existing approaches, which will be demonstrated by our simulation results. The rest of this paper is organized as follows. Section II introduces the preliminaries of this work, including the RS codes and GII-RS codes. Generalization of decoding and the curve-fitting based decoding for GII-RS codes are further proposed in Section III and Section IV, respectively. Simulation results are presented in Section V.

II. Preliminaries

This section presents the preliminaries of RS codes and GII-RS codes, including their encoding and decoding.

A. RS Codes and Curve-Fitting Based Decoding

Let $\mathbb{F}_q = \{0, \alpha^0, \alpha^1, \ldots, \alpha^{q-2}\}$ denote the finite field of size q, where α is a primitive element. Further let $\mathbb{F}_q[x]$ and $\mathbb{F}_q[x, y]$ denote the univariate and bivariate polynomial rings defined over $\mathbb{F}_q$, respectively. In this paper, all polynomials are defined in $\mathbb{F}_q[x]$ or $\mathbb{F}_q[x, y]$. For an (n, k) RS code defined over $\mathbb{F}_q$, where n and k are the length and dimension, respectively, the message $\boldsymbol{u} = [u_0, u_1, \ldots, u_{k-1}] \in \mathbb{F}_q^k$ can

Authorized licensed use limited to: SUN YAT-SEN UNIVERSITY. Downloaded on September 09,2026 at 01:44:23 UTC from IEEE Xplore. Restrictions apply.

be presented as $u(x) = \sum_{j=0}^{k-1} u_j x^j$. Subsequently, codeword $\boldsymbol{c} = [c_0, c_1, \ldots, c_{n-1}] \in \mathbb{F}_q^n$ can be generated by

$$\boldsymbol{c} = [u(\sigma_0), u(\sigma_1), \ldots, u(\sigma_{n-1})], \tag{1}$$

where $\sigma_0, \sigma_1, \ldots, \sigma_{n-1}$ are n distinct nonzero elements of $\mathbb{F}_q$. In maximizing the codeword length, it is often set $n = q - 1$. Similarly, $\boldsymbol{c}$ can be presented as $c(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$. RS codes are also cyclic. Under this paradigm, its generator polynomial can often be defined as

$$g(x) = \prod_{j=1}^{n-k} (x - \alpha^j). \tag{2}$$

Encoding can be realized by

$$c(x) = u(x) g(x). \tag{3}$$

The Guruswami-Sudan (GS) algorithm formulates the decoding as a curve-fitting problem that is capable of yielding a list of codeword estimations. It can correct up to $n - \lfloor \sqrt{n\,(k-1)} \rfloor - 1$ errors [11]. For GS decoding of an (n, k) RS code, the following definition is needed.

Definition I. Given a monomial $x^a y^b$, its $(1, \gamma)$-weighted degree is $\deg_{1,\gamma} x^a y^b = a + \gamma b$. Its lexicographic order is denoted by $\mathrm{ord}(x^a y^b)$. For two distinct monomials $x^{a_1} y^{b_1}$ and $x^{a_2} y^{b_2}$, if $\deg_{1,\gamma} x^{a_1} y^{b_1} > \deg_{1,\gamma} x^{a_2} y^{b_2}$, or $\deg_{1,\gamma} x^{a_1} y^{b_1} = \deg_{1,\gamma} x^{a_2} y^{b_2}$ and $b_1 > b_2$, it is claimed $\mathrm{ord}(x^{a_1} y^{b_1}) > \mathrm{ord}(x^{a_2} y^{b_2})$. Given a polynomial $Q(x, y) = \sum_{a,b} Q_{ab} x^a y^b$, its $(1, \gamma)$-weighted degree and leading order can be defined as $\deg_{1,\gamma} Q(x, y) = \max \{\deg_{1,\gamma} x^a y^b | Q_{ab} \neq 0\}$ and $\mathrm{lod}(Q(x, y)) = \max \{\mathrm{ord}(x^a y^b) | Q_{ab} \neq 0\}$. For two distinct polynomials $Q_1(x, y)$, $Q_2(x, y)$, if $\mathrm{lod}(Q_1(x, y)) > \mathrm{lod}(Q_2(x, y))$, it is claimed $Q_1(x, y) > Q_2(x, y)$. For an (n, k) RS code, $\gamma = k - 1$.

Let $\boldsymbol{r} = [r_0, r_1, \ldots, r_{n-1}] \in \mathbb{F}_q^n$ denote the received word of $\boldsymbol{c}$. Let $d_{\mathrm{H}}(\boldsymbol{c}, \boldsymbol{r})$ denote the Hamming distance between $\boldsymbol{c}$ and $\boldsymbol{r}$. For the decoding, a set of n interpolation points can be formulated as

$$(\sigma_0, r_0), (\sigma_1, r_1), \ldots, (\sigma_{n-1}, r_{n-1}). \tag{4}$$

The GS algorithm constructs a minimal polynomial $Q(x, y)$. It interpolates the above n points with a specified multiplicity m. For a polynomial $Q(x, y) = \sum_{a,b} Q_{ab} x^a y^b$, its $(\mu, \nu)-$Hasse derivative evaluation at point (σ_ψ, r_ψ) is defined as

$$D_{\mu,\nu}^{(\sigma_\psi, r_\psi)} = \sum_{a \geq \mu, b \geq \nu} \binom{a}{\mu} \binom{b}{\nu} Q_{ab} \sigma_\psi^{a-\mu} r_\psi^{b-\nu}, \tag{5}$$

where $\psi = 0, 1, \ldots, n-1$. If $D_{\mu,\nu}^{(\sigma_\psi, r_\psi)} = 0$, $\forall \mu + \nu < m$, then $Q(x, y)$ has an interpolation multiplicity of at least m over the point (σ_ψ, r_ψ). A larger m leads to a stronger error-correction capability, but its decoding is more complex.

Theorem 1 *([11])*. For an (n, k) RS code, let $Q(x, y)$ denote a polynomial that has an interpolation multiplicity of at least m over the points of (4). If

$$m(n - d_{\mathrm{H}}(\boldsymbol{c}, \boldsymbol{r})) > \deg_{1,k-1} Q(x, y), \tag{6}$$

$Q(x, u(x)) = 0$, or equivalently $(y - u(x)) | Q(x, y)$.

Hence, if the decoding succeeds, the message polynomial can be determined by finding y-roots of $Q(x, y)$. Let L denote maximal output list size, where $L = \deg_y Q(x, y)$. In this work, if the output list contains the message $\boldsymbol{u}$, it is considered a successful GS decoding. Among the two decoding steps, interpolation that determines $Q(x, y)$ dominates the complexity. It can be realized by Kötter's algorithm [14], which constructs $Q(x, y)$ in an iterative manner. Kötter's algorithm exhibits complexity of $\mathcal{O}(Lm^4 n^2)$. The root-finding can be realized by Roth-Ruckenstein's algorithm [15].

The KV algorithm is a soft-decision variant of the curve-fitting based decoding. By transforming soft information into the interpolation multiplicities, the decoding performance can be enhanced. Let $\boldsymbol{y} = [y_0, y_1, \ldots, y_{n-1}] \in \mathbb{R}^n$ denote the received symbol vector of codeword $\boldsymbol{c}$. Let $\boldsymbol{\Pi} \in \mathbb{R}^{q \times n}$ denote the reliability matrix of $\boldsymbol{c}$. Its entries are defined as

$$\pi_{\lambda,\psi} = \mathrm{P}(y_\psi | c_\psi = \lambda), \tag{7}$$

where $\lambda \in \mathbb{F}_q$ and $\psi = 0, 1, \ldots, n-1$. With $\boldsymbol{\Pi}$, an interpolation multiplicity matrix $\mathbf{M} \in \mathbb{N}^{q \times n}$ can be derived based on a designed maximal output list size L [16]. Its entry $m_{\lambda,\psi}$ denotes the interpolation multiplicity for point (σ_ψ, λ). Let $S_{\mathrm{M}}(\boldsymbol{c}, \mathbf{M})$ denote the codeword score of the multiplicity matrix $\mathbf{M}$ with respect to $\boldsymbol{c}$, which can be derived as

$$S_{\mathrm{M}}(\boldsymbol{c}, \mathbf{M}) = \sum_{\psi=0}^{n-1} \{m_{\lambda,\psi} | \lambda = c_\psi, \lambda \in \mathbb{F}_q\}. \tag{8}$$

The sufficient condition for a successful decoding of the KV algorithm is defined as follows.

Corollary 2 *([13])*. Given an (n, k) RS code and an interpolation polynomial $Q(x, y)$, if

$$S_{\mathrm{M}}(\boldsymbol{c}, \mathbf{M}) > \deg_{1,k-1} Q(x, y). \tag{9}$$

$Q(x, u(x)) = 0$, or equivalently $(y - u(x)) | Q(x, y)$. Asymptotically when $L = \infty$, inequality (9) can be written as

$$\sum_{\psi=0}^{n-1} \{\pi_{\lambda,\psi} | \lambda = c_\psi, \lambda \in \mathbb{F}_q\} > \sqrt{(k-1) \sum_{\lambda \in \mathbb{F}_q} \sum_{\psi=0}^{n-1} \pi_{\lambda,\psi}^2}. \tag{10}$$

B. GII-RS Codes and Decoding

Let $\{\mathcal{C}_b(n, k_b)\}_{b=0}^{v}$ denote a group of $v + 1$ RS codes that are defined over $\mathbb{F}_q$. Among them, $\mathcal{C}_0(n, k_0)$ is the front layer RS code and $\mathcal{C}_b(n, k_b)$ is the b-th nested layer RS code, where $b = 1, 2, \ldots, v$. Note that they exhibit a nested structure such that $\mathcal{C}_v \subseteq \mathcal{C}_{v-1} \subseteq \ldots \subseteq \mathcal{C}_0$, and hence $k_0 \geq k_1 \geq \ldots \geq k_v$. Let d_b denote the minimum Hamming distance of $\mathcal{C}_b(n, k_b)$ and t_b denote its error-correction capability. They satisfy $d_0 \leq d_1 \leq \ldots \leq d_v$ and $t_0 \leq t_1 \leq \ldots \leq t_v$. A $([\rho, v], n)$ GII-RS code consists of ρ interleaves $\boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_{\rho-1} \in \mathcal{C}_0(n, k_0)$, where $\rho \geq v$. Their linear combinations produce v nested codewords

Authorized licensed use limited to: SUN YAT-SEN UNIVERSITY. Downloaded on September 09,2026 at 01:44:23 UTC from IEEE Xplore. Restrictions apply.

$\tilde{\boldsymbol{c}}_0 \in \mathcal{C}_v(n,k_v), \tilde{\boldsymbol{c}}_1 \in \mathcal{C}_{v-1}(n,k_{v-1}), \ldots, \tilde{\boldsymbol{c}}_{v-1} \in \mathcal{C}_1(n,k_1)$. This can be characterized by

$$\begin{bmatrix} \tilde{\boldsymbol{c}}_0 \\ \tilde{\boldsymbol{c}}_1 \\ \vdots \\ \tilde{\boldsymbol{c}}_{v-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha & \cdots & \alpha^{\rho-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{v-1} & \cdots & \alpha^{(v-1)(\rho-1)} \end{bmatrix} \begin{bmatrix} \boldsymbol{c}_0 \\ \boldsymbol{c}_1 \\ \vdots \\ \boldsymbol{c}_{\rho-1} \end{bmatrix}. \tag{11}$$

This GII-RS code has a length of $N = \rho n$ and a dimension of $K = (\rho - v)k_0 + k_1 + k_2 + \ldots + k_v$, respectively. The message of the GII-RS code can be denoted as $\boldsymbol{u}_{\mathrm{G}} = [\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_{\rho-1}] \in \mathbb{F}_q^K$, where $\boldsymbol{u}_0 \in \mathbb{F}_q^{k_v}, \boldsymbol{u}_1 \in \mathbb{F}_q^{k_{v-1}}, \ldots, \boldsymbol{u}_{v-1} \in \mathbb{F}_q^{k_1}$ and $\boldsymbol{u}_v, \ldots, \boldsymbol{u}_{\rho-1} \in \mathbb{F}_q^{k_0}$, respectively. A $([\rho, v], n)$ GII codeword can be denoted as $\boldsymbol{c}_{\mathrm{G}} = [\boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_{\rho-1}] \in \mathbb{F}_q^{\rho n}$. The existing BM decoding of GII-RS codes was proposed in [1]. Higher order syndromes can be computed by (11), effectively correcting more error patterns that cannot be decoded by only the front layer codes.

III. Generalization of Decoding

For a $([\rho, v], n)$ GII-RS code, its subsequent received word can be denoted as $\boldsymbol{r}_{\mathrm{G}} = [\boldsymbol{r}_0, \boldsymbol{r}_1, \ldots, \boldsymbol{r}_{\rho-1}] \in \mathbb{F}_q^{\rho n}$, where $\boldsymbol{r}_0, \boldsymbol{r}_1, \ldots, \boldsymbol{r}_{\rho-1} \in \mathbb{F}_q^n$ are the variants of $\boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_{\rho-1}$, respectively. Decoding can be divided into at most $v+1$ stages. In this work, the decoding stage is defined by the number of remaining interleaves that have not been successfully decoded. The decoding starts with stage-0, during which the ρ interleaves can be decoded in parallel. Afterwards, if the number of interleaves that have not been successfully decoded exceeds v, decoding fails. Note that based on (11), we can apply at most v nested codewords for assisting the recovery of the interleaves. Otherwise, the decoding proceeds to the next stage. In decoding stage-b, where $b = 1, 2, \ldots, v$, there are $v-b+1$ interleaves that have not been successfully decoded. Let $\mathcal{L} = \{l_0, l_1, \ldots, l_{v-b}\}$ denote the index set of the $v-b+1$ remaining received words. Hence, its complementary set $\mathcal{L}^{\mathrm{c}} = \{0, 1, \ldots, \rho-1\} \backslash \mathcal{L}$ denotes the interleaves that have been decoded. The remaining received words are denoted as

$$\boldsymbol{r}_{l_0} = \boldsymbol{c}_{l_0} + \boldsymbol{e}_{l_0}, \boldsymbol{r}_{l_1} = \boldsymbol{c}_{l_1} + \boldsymbol{e}_{l_1}, \ldots, \boldsymbol{r}_{l_{v-b}} = \boldsymbol{c}_{l_{v-b}} + \boldsymbol{e}_{l_{v-b}}. \tag{12}$$

The error patterns of the remaining received words can be projected onto the nested codebook $\mathcal{C}_b$, instead of (12) as the ones superimposed onto codewords of $\mathcal{C}_0$, through reconstructing new received words. Note that $\mathcal{C}_b$ has a stronger error-correction capability than $\mathcal{C}_0$. Let $\dot{\boldsymbol{r}}_0, \dot{\boldsymbol{r}}_1, \ldots, \dot{\boldsymbol{r}}_{v-b} \in \mathbb{F}_q^n$ denote the reconstructed new received words as

$$\dot{\boldsymbol{r}}_0 = \dot{\boldsymbol{c}}_0 + \boldsymbol{e}_{l_0}, \dot{\boldsymbol{r}}_1 = \dot{\boldsymbol{c}}_1 + \boldsymbol{e}_{l_1}, \ldots, \dot{\boldsymbol{r}}_{v-b} = \dot{\boldsymbol{c}}_{v-b} + \boldsymbol{e}_{l_{v-b}}, \tag{13}$$

where codewords $\dot{\boldsymbol{c}}_0, \dot{\boldsymbol{c}}_1, \ldots, \dot{\boldsymbol{c}}_{v-b} \in \mathcal{C}_b$. Let us define a Vandermonde matrix $\boldsymbol{\Upsilon}$ as

$$\boldsymbol{\Upsilon} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{l_0} & \alpha^{l_1} & \cdots & \alpha^{l_{v-b}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{(v-b)l_0} & \alpha^{(v-b)l_1} & \cdots & \alpha^{(v-b)l_{v-b}} \end{bmatrix}, \tag{14}$$

where $\boldsymbol{\Upsilon} \in \mathbb{F}_q^{(v-b+1)\times(v-b+1)}$. Let us further define matrix $\boldsymbol{\Theta}$ as in (15), where $\boldsymbol{\Theta} \in \mathbb{F}_q^{(v-b+1)\times(\rho-v+b-1)}$. Let $\boldsymbol{s}_0, \boldsymbol{s}_1, \ldots, \boldsymbol{s}_{v-b} \in \mathcal{C}_0$ denote codewords which satisfy

$$\begin{aligned} &[\boldsymbol{s}_0, \boldsymbol{s}_1, \ldots, \boldsymbol{s}_{v-b}\ ]^{\mathrm{T}} = \boldsymbol{\Upsilon}^{-1}\boldsymbol{\Theta} \\ &[\boldsymbol{c}_0, \ldots, \boldsymbol{c}_{l_0-1}, \boldsymbol{c}_{l_0+1}, \ldots, \boldsymbol{c}_{l_1-1}, \boldsymbol{c}_{l_1+1}, \ldots, \boldsymbol{c}_{\rho-1}]^{\mathrm{T}}, \end{aligned} \tag{16}$$

where T denotes transposition of the matrix. The following theorem shows that $\dot{\boldsymbol{r}}_0, \dot{\boldsymbol{r}}_1, \ldots, \dot{\boldsymbol{r}}_{v-b}$ can be determined by $\boldsymbol{s_0}, \boldsymbol{s}_1, \ldots, \boldsymbol{s}_{v-b}$.

Theorem 3. For $\boldsymbol{r}_{l_0}, \boldsymbol{r}_{l_1}, \ldots, \boldsymbol{r}_{l_{v-b}}$, their reconstructed received words $\dot{\boldsymbol{r}}_0, \dot{\boldsymbol{r}}_1, \ldots, \dot{\boldsymbol{r}}_{v-b}$ can be determined as

$$\begin{bmatrix} \dot{\boldsymbol{r}}_0 \\ \dot{\boldsymbol{r}}_1 \\ \vdots \\ \dot{\boldsymbol{r}}_{v-b} \end{bmatrix} = \begin{bmatrix} \boldsymbol{r}_{l_0} \\ \boldsymbol{r}_{l_1} \\ \vdots \\ \boldsymbol{r}_{l_{v-b}} \end{bmatrix} + \begin{bmatrix} \boldsymbol{s}_0 \\ \boldsymbol{s}_1 \\ \vdots \\ \boldsymbol{s}_{v-b} \end{bmatrix}. \tag{17}$$

Proof: Let $\tilde{\boldsymbol{r}}_0, \tilde{\boldsymbol{r}}_1, \ldots, \tilde{\boldsymbol{r}}_{v-b} \in \mathbb{F}_q^n$ denote the nested received words that are determined from the ρ received words through (11). That says

$$\begin{bmatrix} \tilde{\boldsymbol{r}}_0 \\ \tilde{\boldsymbol{r}}_1 \\ \vdots \\ \tilde{\boldsymbol{r}}_{v-b} \end{bmatrix} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha & \cdots & \alpha^{\rho-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{v-b} & \cdots & \alpha^{(v-b)(\rho-1)} \end{bmatrix} \begin{bmatrix} \boldsymbol{r}_0 \\ \boldsymbol{r}_1 \\ \vdots \\ \boldsymbol{r}_{\rho-1} \end{bmatrix}. \tag{18}$$

Let $\tilde{\boldsymbol{e}}_0, \tilde{\boldsymbol{e}}_1, \ldots, \tilde{\boldsymbol{e}}_{v-b} \in \mathbb{F}_q^n$ denote the corresponding nested error patterns, which are

$$\begin{bmatrix} \tilde{\boldsymbol{e}}_0 \\ \tilde{\boldsymbol{e}}_1 \\ \vdots \\ \tilde{\boldsymbol{e}}_{v-b} \end{bmatrix} = \boldsymbol{\Upsilon} \begin{bmatrix} \boldsymbol{e}_{l_0} \\ \boldsymbol{e}_{l_1} \\ \vdots \\ \boldsymbol{e}_{l_{v-b}} \end{bmatrix}. \tag{19}$$

The nested received words of (18) can be written as

$$\begin{bmatrix} \tilde{\boldsymbol{r}}_0 \\ \tilde{\boldsymbol{r}}_1 \\ \vdots \\ \tilde{\boldsymbol{r}}_{v-b} \end{bmatrix} = \begin{bmatrix} \tilde{\boldsymbol{c}}_0 \\ \tilde{\boldsymbol{c}}_1 \\ \vdots \\ \tilde{\boldsymbol{c}}_{v-b} \end{bmatrix} + \begin{bmatrix} \tilde{\boldsymbol{e}}_0 \\ \tilde{\boldsymbol{e}}_1 \\ \vdots \\ \tilde{\boldsymbol{e}}_{v-b} \end{bmatrix}. \tag{20}$$

Based on (11) and since $\mathcal{C}_v \subseteq \mathcal{C}_{v-1} \subseteq \ldots \subseteq \mathcal{C}_b \subseteq \ldots \subseteq \mathcal{C}_0$, $\tilde{\boldsymbol{c}}_0, \tilde{\boldsymbol{c}}_1, \ldots, \tilde{\boldsymbol{c}}_{v-b} \in \mathcal{C}_b$. Assume that $\dot{\boldsymbol{c}}_0, \dot{\boldsymbol{c}}_1, \ldots, \dot{\boldsymbol{c}}_{v-b}$ satisfy

$$\begin{bmatrix} \tilde{\boldsymbol{c}}_0 \\ \tilde{\boldsymbol{c}}_1 \\ \vdots \\ \tilde{\boldsymbol{c}}_{v-b} \end{bmatrix} = \boldsymbol{\Upsilon} \begin{bmatrix} \dot{\boldsymbol{c}}_0 \\ \dot{\boldsymbol{c}}_1 \\ \vdots \\ \dot{\boldsymbol{c}}_{v-b} \end{bmatrix}. \tag{21}$$

Therefore, based on (19) and (21), (20) can be written as

$$\begin{bmatrix} \tilde{\boldsymbol{r}}_0 \\ \tilde{\boldsymbol{r}}_1 \\ \vdots \\ \tilde{\boldsymbol{r}}_{v-b} \end{bmatrix} = \boldsymbol{\Upsilon} \begin{bmatrix} \dot{\boldsymbol{c}}_0 \\ \dot{\boldsymbol{c}}_1 \\ \vdots \\ \dot{\boldsymbol{c}}_{v-b} \end{bmatrix} + \boldsymbol{\Upsilon} \begin{bmatrix} \boldsymbol{e}_{l_0} \\ \boldsymbol{e}_{l_1} \\ \vdots \\ \boldsymbol{e}_{l_{v-b}} \end{bmatrix}. \tag{22}$$

Based on (13), the reconstructed received words can be deter-

Authorized licensed use limited to: SUN YAT-SEN UNIVERSITY. Downloaded on September 09,2026 at 01:44:23 UTC from IEEE Xplore. Restrictions apply.

$$\boldsymbol{\Theta}=\begin{bmatrix} 1 & \cdots & 1 & 1 & \cdots & 1 & 1 & \cdots & 1 \\ \alpha & \cdots & \alpha^{l_0-1} & \alpha^{l_0+1} & \cdots & \alpha^{l_1-1} & \alpha^{l_1+1} & \cdots & \alpha^{\rho-1} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \alpha^{v-b} & \cdots & \alpha^{(v-b)(l_0-1)} & \alpha^{(v-b)(l_0+1)} & \cdots & \alpha^{(v-b)(l_1-1)} & \alpha^{(v-b)(l_1+1)} & \cdots & \alpha^{(v-b)(\rho-1)} \end{bmatrix}, \tag{15}$$

mined by

$$\begin{bmatrix} \dot{\boldsymbol{r}}_0 \\ \dot{\boldsymbol{r}}_1 \\ \vdots \\ \dot{\boldsymbol{r}}_{v-b} \end{bmatrix} = \boldsymbol{\Upsilon}^{-1} \begin{bmatrix} \tilde{\boldsymbol{r}}_0 \\ \tilde{\boldsymbol{r}}_1 \\ \vdots \\ \tilde{\boldsymbol{r}}_{v-b} \end{bmatrix}. \tag{23}$$

Based on (18), (23) can be further rewritten as

$$\begin{bmatrix} \dot{\boldsymbol{r}}_0 \\ \dot{\boldsymbol{r}}_1 \\ \vdots \\ \dot{\boldsymbol{r}}_{v-b} \end{bmatrix} = \boldsymbol{\Upsilon}^{-1} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha & \cdots & \alpha^{\rho-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{v-b} & \cdots & \alpha^{(v-b)(\rho-1)} \end{bmatrix} \begin{bmatrix} \boldsymbol{r}_0 \\ \boldsymbol{r}_1 \\ \vdots \\ \boldsymbol{r}_{\rho-1} \end{bmatrix}. \tag{24}$$

Substituting (14) and (15) into (24) leads to (17). □

Based on Theorem 3, error pattern $\boldsymbol{e}_{l_j}$ of the remaining interleave $\boldsymbol{c}_{l_j} \in \mathcal{C}_0$ can be projected onto the nested codebook $\mathcal{C}_b$ with a stronger error-correction capability.

IV. Curve-Fitting Based Decoding

Theorem 3 shows that error patterns of the corrupted interleaves can be projected onto the nested codebook as being superimposed onto its codewords. The curve-fitting based decoding can be employed to determine the error patterns. This section proposes the hard-decision approach, i.e., the GS algorithm, and the soft-decision approach, i.e., the KV algorithm, for decoding GII-RS codes.

A. Hard-Decision Approach

Since the codebook onto which the error patterns are projected varies across different stages, the interpolation multiplicity can be assigned stage wise. Let m_b denote the interpolation multiplicity of stage-b. In stage-0, given the received word $\boldsymbol{r}_{\mathrm{G}} = [\boldsymbol{r}_0, \boldsymbol{r}_1, \ldots, \boldsymbol{r}_{\rho-1}] \in \mathbb{F}_q^{\rho n}$ of a $([\rho, v], n)$ GII-RS code, ρ received words are decoded by the GS algorithm with a multiplicity of m_0. The interpolation points of the received word $\boldsymbol{r}_i = [r_0^{(i)}, r_1^{(i)}, \ldots, r_{n-1}^{(i)}]$ can be written as

$$(\sigma_0, r_0^{(i)}), (\sigma_1, r_1^{(i)}), \ldots, (\sigma_{n-1}, r_{n-1}^{(i)}), \tag{25}$$

where $i = 0, 1, \ldots, \rho-1$. The GS algorithm constructs a minimal polynomial $Q_0^{(i)}(x, y)$ which has an interpolation multiplicity of at least m_0 over all the above n points. Based on Theorem 1, if $Q_0^{(i)}(x, y)$ satisfies

$$m_0(n - d_{\mathrm{H}}(\boldsymbol{c}_i, \boldsymbol{r}_i)) > \deg_{1,k_0-1} Q_0^{(i)}(x, y), \tag{26}$$

the message $\boldsymbol{u}_i$ can be determined by finding y-roots of $Q_0^{(i)}(x, y)$. If all interleaves are decoded, the decoding will be terminated. Otherwise, the decoding proceeds to next stage.

Without loss of generality, in stage-b, the remaining received words $\boldsymbol{r}_{l_0}, \boldsymbol{r}_{l_1}, \ldots, \boldsymbol{r}_{l_{v-b}}$ are further decoded. Based on Theorem 3, error pattern $\boldsymbol{e}_{l_j}$ can be projected onto the nested codebook $\mathcal{C}_b$ by reconstructing $\dot{\boldsymbol{r}}_j = \dot{\boldsymbol{c}}_j + \boldsymbol{e}_{l_j}$. The GS algorithm can be applied to decode $\dot{\boldsymbol{r}}_j$, thereby determining $\boldsymbol{e}_{l_j}$, where $j = 0, 1, \ldots, v-b$. The interpolation points of $\dot{\boldsymbol{r}}_j = [\dot{r}_0^{(j)}, \dot{r}_1^{(j)}, \ldots, \dot{r}_{n-1}^{(j)}]$ can again be formulated as

$$(\sigma_0, \dot{r}_0^{(j)}), (\sigma_1, \dot{r}_1^{(j)}), \ldots, (\sigma_{n-1}, \dot{r}_{n-1}^{(j)}). \tag{27}$$

The GS algorithm constructs a minimal polynomial $Q_b^{(j)}(x, y)$ which has an interpolation multiplicity of at least m_b over all the above n points. Let $\dot{\boldsymbol{u}}_j \in \mathbb{F}_q^{k_b}$ denote the message of $\dot{\boldsymbol{c}}_j$. Again, if

$$m_b(n - d_{\mathrm{H}}(\dot{\boldsymbol{c}}_j, \dot{\boldsymbol{r}}_j)) > \deg_{1,k_b-1} Q_b^{(j)}(x, y), \tag{28}$$

$\dot{\boldsymbol{u}}_j$ can be retrieved by finding y-roots of $Q_b^{(j)}(x, y)$, thereby determining $\dot{\boldsymbol{c}}_j$ and $\boldsymbol{e}_{l_j}$. Therefore, interleave $\boldsymbol{c}_{l_j}$ can be recovered by $\boldsymbol{c}_{l_j} = \boldsymbol{r}_{l_j} + \boldsymbol{e}_{l_j}$. Since the nested codebook $\mathcal{C}_b$ has a lower dimension than $\mathcal{C}_0$, the GS algorithm often exhibits a more competent error-correction capability than the BM algorithm. Let L_b denote the maximum decoding output list size in stage-b. There are at most $v+1$ decoding stages in a GII-RS code. The worst case decoding complexity can be characterized as $\mathcal{O}(n^2(\rho {m_0}^4 L_0 + v{m_1}^4 L_1 + (v-1){m_2}^4 L_2 + \ldots + {m_v}^4 L_v))$. Let $\mathcal{L}'$ denote a backup of $\mathcal{L}$. The above introduced GS decoding of GII-RS codes is summarized as in Algorithm 1.

B. Soft-Decision Approach

The KV algorithm can be applied to further enhance the error-correction capability in each decoding stage. In stage-0, let $\boldsymbol{y}_i = [y_0^{(i)}, y_1^{(i)}, \ldots, y_{n-1}^{(i)}] \in \mathbb{R}^n$ denote the received symbol vector of interleave $\boldsymbol{c}_i = [c_0^{(i)}, c_1^{(i)}, \ldots, c_{n-1}^{(i)}]$. Its reliability matrix can be denoted as $\boldsymbol{\Pi}^{(i)} \in \mathbb{R}^{q \times n}$, where $i = 0, 1, \cdots, \rho-1$. Its entries are defined as

$$\pi_{\lambda,\psi}^{(i)} = \mathrm{P}(y_\psi^{(i)} | c_\psi^{(i)} = \lambda), \tag{29}$$

where $\lambda \in \mathbb{F}_q$ and $\psi = 0, 1, \ldots, n-1$. Let $\mathbf{M}^{(i)} \in \mathbb{N}^{q \times n}$ denote the corresponding multiplicity matrix, where its entry $m_{\lambda,\psi}^{(i)}$ denotes the interpolation multiplicity for point (σ_ψ, λ).

For reconstructed codeword $\dot{\boldsymbol{c}}_j = [\dot{c}_0^{(j)}, \dot{c}_1^{(j)}, \ldots, \dot{c}_{n-1}^{(j)}]$ in stage-b, where $j = 0, 1, \ldots, v-b$, the reliability matrix is denoted as $\dot{\boldsymbol{\Pi}}^{(j)} \in \mathbb{N}^{q \times n}$ with entries $\dot{\pi}_{\lambda,\psi}^{(j)}$ defined as

$$\dot{\pi}_{\lambda,\psi}^{(j)} = \mathrm{P}(y_\psi^{(l_j)} | \dot{c}_\psi^{(j)} = \lambda). \tag{30}$$

Based on (17), given $\boldsymbol{s}_j = [s_0^{(j)}, s_1^{(j)}, \ldots, s_{n-1}^{(j)}]$, the following

Authorized licensed use limited to: SUN YAT-SEN UNIVERSITY. Downloaded on September 09,2026 at 01:44:23 UTC from IEEE Xplore. Restrictions apply.

Algorithm 1: GS Decoding of GII-RS Codes

Input: $\boldsymbol{r}_{\mathrm{G}} = [\boldsymbol{r}_0, \boldsymbol{r}_1, \ldots, \boldsymbol{r}_{\rho-1}]$ and $m_0, m_1, \ldots, m_v$;
Initialize $\mathcal{L} = \mathcal{L}' = \emptyset, b = 0$;
For $i = 0, 1, \ldots, \rho - 1$ **do**
  Construct $Q_0^{(i)}(x, y)$ with m_0 ;
  Determine $\boldsymbol{u}_i$;
  If decoding fails **then**
    $\mathcal{L} = \mathcal{L} \cup \{i\}$;
If $|\mathcal{L}| > v$ **then**
  Declare a decoding failure;
While $\mathcal{L} \neq \emptyset$ **do**
  $b = v - |\mathcal{L}| + 1$;
  Compute reconstructed received words $\dot{\boldsymbol{r}}_0, \dot{\boldsymbol{r}}_1, \ldots, \dot{\boldsymbol{r}}_{|\mathcal{L}|-1}$ as in (17);
  Let $\mathcal{L}' = \mathcal{L}$, $\mathcal{L} = \emptyset$;
  For $j \in \mathcal{L}$ **do**
    Construct $Q_b^{(j)}(x, y)$ with m_b ;
    Determine $\dot{\boldsymbol{u}}_j$, $\dot{\boldsymbol{c}}_j$ and $\boldsymbol{e}_{l_j}$;
    If the decoding fails **then**
      $\mathcal{L} = \mathcal{L} \cup \{j\}$;
    Else
      $\boldsymbol{c}_j = \boldsymbol{r}_j + \boldsymbol{e}_j$;
  If $|\mathcal{L}| = |\mathcal{L}'|$ **then**
    Declare a decoding failure;

theorem shows that columns of $\dot{\mathbf{\Pi}}^{(j)}$ are the symbol wise reshuffle of those of $\mathbf{\Pi}^{(l_j)}$.

Theorem 4. Reliability matrix $\dot{\mathbf{\Pi}}^{(j)}$ can be generated by performing symbol wise reshuffle on columns of $\mathbf{\Pi}^{(l_j)}$ as

$$\dot{\pi}_{\lambda,\psi}^{(j)} = \pi_{\lambda+s_{\psi}^{(j)},\psi}^{(l_j)}. \tag{31}$$

Proof: Based on (17), $\dot{\pi}_{\lambda,\psi}^{(j)}$ can be given by

$$\begin{aligned}\dot{\pi}_{\lambda,\psi}^{(j)} &= \mathrm{P}(y_{\psi}^{(l_j)} | \dot{c}_{\psi}^{(j)} = \lambda) \\ &= \mathrm{P}(y_{\psi}^{(l_j)} | c_{\psi}^{(l_j)} = \lambda + s_{\psi}^{(j)}) \\ &= \pi_{\lambda+s_{\psi}^{(j)},\psi}^{(l_j)}.\end{aligned}$$

□

Based on Theorem 4, $\dot{\mathbf{\Pi}}^{(j)}$ can be uniquely determined by $\mathbf{\Pi}^{(l_j)}$. Let $\dot{\mathbf{M}}^{(j)} \in \mathbb{N}^{q \times n}$ denote the multiplicity matrix for decoding $\dot{\boldsymbol{r}}_j$, where its entry $\dot{m}_{\lambda,\psi}^{(j)}$ denotes the interpolation multiplicity for point (σ_ψ, λ). Given a designed maximum decoding output list size L, the multiplicity matrices $\mathbf{M}^{(i)}$ and $\dot{\mathbf{M}}^{(j)}$ can be generated from $\mathbf{\Pi}^{(i)}$ and $\dot{\mathbf{\Pi}}^{(j)}$ [16], respectively. A larger L leads to a stronger error-correction capability, but its decoding is more complex.

V. Simulation Results

This section presents decoding performance of GII-RS codes over the additive white Gaussian noise (AWGN) channel, which are obtained using binary phase shift keying (BPSK) modulation. Let N_0 denote the single side-band power spectrum density of the channel. Signal-to-noise ratio (SNR) is defined as E_{b}/N_0, where E_{b} is the transmitted energy per information bit. Decoding frame error rate (FER) is evaluated and the coding gains are measured at the decoding FER of 10^{-4}. Fig. 1 compares the decoding performance of the concatenating multiple RS codes (including the (63,39), (63,19), (63,17), and (63,15) RS codes), the (255, 83) RS code and the ([4,3], 63) GII-RS code. They all have similar length (symbol wise) and rate. The decoding failure of any single code constitutes a decoding failure for the entire set of multiple RS codes. Multiple RS codes mentioned above can be integrated in forming a ([4, 3], 63) GII-RS code which yields remarkable performance improvements. Note that for the GS decoding, it is set $m_0 = m_1 = m_2 = m_3 = 1$. It can be seen that GS decoding of the GII code yields a coding gain of 0.32 dB over the existing BM decoding, which also yields a coding gain of 0.10 dB over GS decoding of the (255, 83) RS code. When $L = 6$, the KV decoding yields a coding gain of 0.12 dB over GS decoding of the GII-RS code. When $L \leftarrow \infty$, the optimal KV decoding yields a coding gain of 1.04 dB over GS decoding of the GII-RS code. This reveals the decoding performance potential for the GII-RS codes. Note that the optimal KV decoding performance is obtained by assessing the inequality of (10), without conducting interpolation and root-finding. Finally, it should also be pointed out that parameters of both the GS decoding and KV decoding can be adjusted in a stage wise manner, potentially resulting in a better decoding performance-complexity tradeoff, as well be conducted in our future works.

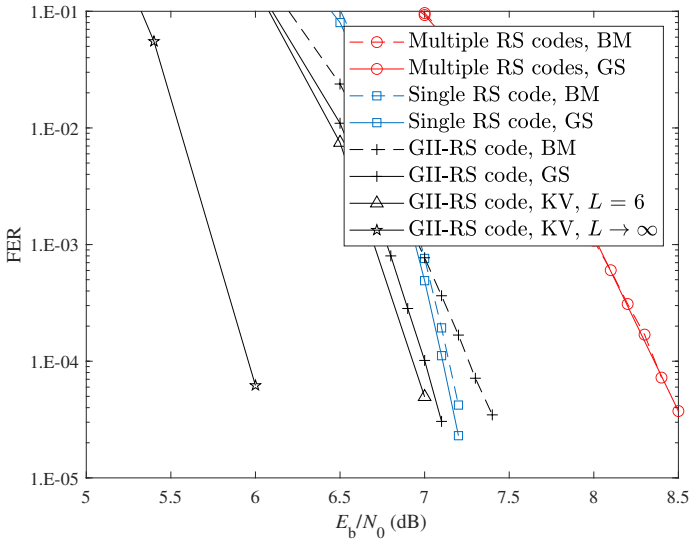

Fig. 1. Comparison between the RS codes and GII-RS codes.

Acknowledgment

This work is supported in part by the National Natural Science Foundation of China (NSFC) with project ID 62471503; and in part by the Natural Science Foundation of Guangdong Province with project ID 2024A1515010213.

Authorized licensed use limited to: SUN YAT-SEN UNIVERSITY. Downloaded on September 09,2026 at 01:44:23 UTC from IEEE Xplore. Restrictions apply.

REFERENCES

[1] Y. Wu, "Generalized integrated interleaved codes," *IEEE Trans. Inf. Theory*, vol. 63, no. 2, pp. 1102–1119, Feb. 2017.

[2] J. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inf. Theory*, vol. 15, no. 1, pp. 122–127, Jan. 1969.

[3] Z. Xie and X. Zhang, "Fast nested key equation solvers for generalized integrated interleaved decoder," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 68, no. 1, pp. 483–495, Jan. 2021.

[4] W. Li, J. Tian, J. Lin and *et al.*, "Modified GII-BCH codes for low-complexity and low-latency encoders," *IEEE Commun. Lett.*, vol. 23, no. 5, pp. 785–788, May 2019.

[5] Y. Wu, "High-speed LFSR decoder architectures for BCH and GII codes," *IEEE J. Sel. Areas Inf. Theory*, vol. 4, pp. 331–350, Aug. 2023.

[6] Z. Xie and X. Zhang, "Reduced-complexity key equation solvers for generalized integrated interleaved BCH decoders," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 67, no. 12, pp. 5520–5529, Dec. 2020.

[7] Y. J. Tang and X. Zhang, "Fast and low-complexity soft-decision generalized integrated interleaved decoder," *IEEE J. Sel. Areas Inf. Theory*, vol. 4, pp. 174–189, Jul. 2023.

[8] X. He, L. Chen, and Y. Wu, "Performance analysis and enhanced Chase decoding of GII-BCH codes," *IEEE Trans. Commun.*, vol. 73, no. 10, pp. 8647–8658, Oct. 2025.

[9] X. Zhang and Z. Xie, "Efficient architectures for generalized integrated interleaved decoder," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 66, no. 10, pp. 4018–4031, Oct. 2019.

[10] H. Cui, S. Song, and Z. Wang, "An improved method for performance analysis of generalized integrated interleaved codes," *IEEE Commun. Lett.*, vol. 25, no. 10, pp. 3166–3169, Oct. 2021.

[11] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon and algebraic-geometry codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1757–1767, Sep. 1999.

[12] D. Chase, "Class of algorithms for decoding block codes with channel measurement information," *IEEE Trans. Inf. Theory*, vol. 18, no. 1, pp. 170–182, Jan. 1972.

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

[14] R. Kötter, "On algebraic decoding of algebraic-geometric and cyclic codes," Ph.D. dissertation, Linköping Uni., Linköping, Sweden, 1996, dept. Electr. Eng.

[15] R. Roth and G. Ruckenstein, "Efficient decoding of Reed-Solomon codes beyond half the minimum distance," *IEEE Trans. Inf. Theory*, vol. 46, no. 1, pp. 246–257, 2000.

[16] L. Chen, R. Carrasco, and M. Johnston, "Soft-decision list decoding of Hermitian codes," *IEEE Trans. Commun.*, vol. 57, no. 8, pp. 2169–2176, Aug. 2009.

Authorized licensed use limited to: SUN YAT-SEN UNIVERSITY. Downloaded on September 09,2026 at 01:44:23 UTC from IEEE Xplore. Restrictions apply.