On the Error-Correcting Radius of Folded Reed–Solomon Code Designs

Joschi Brauchle

Abstract A general formula for the error-correcting radius of linear-algebraic multivariate interpolation decoding of folded Reed–Solomon (FRS) codes is derived. Based on this result, an improved construction of FRS codes is motivated, which can be obtained by puncturing Parvaresh–Vardy codes. The proposed codes allow decoding for all rates, remove the structural loss in decoding radius of the original FRS design and maximize the fraction of correctable errors.

Key words: Decoding Radius, Low-Order Folded Reed–Solomon Codes, Multivariate Interpolation, Parvaresh–Vardy Codes

1 Introduction

Decoding Reed–Solomon (RS) codes can be seen as reconstructing a message polynomial of limited degree from a set of noisy evaluation points. There exist a multitude of univariate and multivariate interpolation decoding (MID) algorithms solving this problem. The classical bounded minimum distance decoder of Berlekamp–Welch (BW) [11] can be interpreted [1, 6] as a starting point for most MID algorithms. For an RS code of rate R the BW decoder recovers a list-of-1 candidate polynomial at minimum Hamming distance from the received word up to a fraction of $(1-R)/2$ errors. Extending this idea, Sudan in [9] allowed for a list of $l \geq 1$ candidate polynomials to be recovered up to a radius of $1-\sqrt{2R}$ via bivariate interpolation. Guruswami–Sudan [3] increased the radius to $1-\sqrt{R}$ by means of multiplicities of the interpolation points. Parvaresh–Vardy (PV) codes [8] improve upon this value using MID of multiple algebraically correlated polynomials.

Simple linear-algebraic decoding of ℓ-order PV codes allows to correct up to a fraction of $\ell/(\ell+1)(1-\ell R)$ errors, but with a strong rate limitation. Through a

Joschi Brauchle, e-mail: joschi.brauchle@tum.de
Institute for Communications Engineering, Technische Universität München, Munich, Germany

puncturing pattern, Guruswami–Rudra [2] deduced m-folded Reed–Solomon (FRS) codes from PV codes which are linear-algebraically decodable [10] up to a fraction of $s/(s+1)(1-mR/(m-s+1))$ errors with a lesser rate restriction. By allowing higher degree interpolation and interpolation points with multiplicities (which shall not be considered here for the sake of simple linear-algebraic decoding), a fraction of $1-(mR/(m-s+1))^{s/(s+1)}$ errors may be corrected using these codes.

In this paper, a general formula for the decoding radius of linear-algebraic MID in terms of code and decoder parameters is derived, showing that FRS codes are not designed optimally. An improved version called "low-order" m-folded Reed–Solomon (LOFRS) codes with a decoding radius up to $m/(m+1)(1-R)$ is motivated by this result. The term LOFRS was coined in a recent paper by Guruswami–Wang [4], who present a similar design that we wish to explicitly acknowledge. The contribution of this paper is to present LOFRS codes from a different perspective and to illustrate their relationship to PV codes.

The paper is organized as follows. Section 2 introduces notation and defines RS, PV and FRS codes. In Section 3, a general formula for the decoding radius of linear-algebraic MID is derived and applied to RS, PV and FRS codes. Section 4 analyzes the parameters of this formula such that an optimal decoding radius is achieved. It is shown that FRS codes can not make use of these parameters, so an improved design for FRS codes is presented and evaluated. Section 5 concludes the paper.

2 Review of (Folded) Reed–Solomon and Parvaresh–Vardy Codes

Let $\mathbb{F}_q$ be a finite field of order q, and $\mathbb{F}_q^* \coloneqq \mathbb{F}_q \backslash \{0\}$ its multiplicative group with generating element $\alpha \in \mathbb{F}_q^*$. A vector space of dimension ℓ over $\mathbb{F}_q$ is denoted by $\mathbb{F}_q^\ell$ and the ring of polynomials in indeterminate x with coefficients in $\mathbb{F}_q$ by $\mathbb{F}_q[x]$. Let $\mathbb{F}_q[x]_{<k} \coloneqq \left\{ f \in \mathbb{F}_q[x] : \deg f < k \right\}$ be the vector space of polynomials in $\mathbb{F}_q[x]$ of degree less than k. The set of integers $\{1,\dots,n\} =: [1,n]$ and let $\mathscr{E}(j,i,\ell) \coloneqq \left\{ \alpha^j, \alpha^{j+i}, \dots, \alpha^{j+i(\ell-1)} \right\}$ be an ordered set of ℓ distinct multiples of α^i, starting at α^j.

Definition 1 (Evaluation Map). The evaluation map $\mathrm{ev}_{\mathscr{E}(j,i,\ell)} : \mathbb{F}_q[x]_{<k} \to \mathbb{F}_q^\ell$ is defined as $f \mapsto \left(f\left(\alpha^j\right), f\left(\alpha^{j+i}\right), \dots, f\left(\alpha^{j+(\ell-1)i}\right) \right)$.

Definition 2 (Reed–Solomon Code). Let $\mathscr{E}$ be an evaluation set of n distinct elements from $\mathbb{F}_q$ called *code locators*. A RS code of length $n = |\mathscr{E}|$ and dimension $k \in [1,n]$ is the image of all message polynomials $f(x) = f_0 + f_1 x + \dots + f_{k-1}x^{k-1} \in \mathbb{F}_q[x]_{<k}$ under the evaluation map $\mathrm{ev}_{\mathscr{E}}$, i.e.,

$$\mathrm{RS}[q, \mathscr{E}, k] \coloneqq \left\{ (\mathrm{ev}_{\mathscr{E}}(f)) : \forall f \in \mathbb{F}_q[x]_{<k} \right\} \tag{1}$$

and rate $R_{\mathrm{RS}} = k/n =: R$. If $\mathscr{E} = \mathbb{F}_q^*$, $n = |\mathbb{F}_q^*| = q-1$, the code is called *primitive*.

In this paper, all considered RS codes are primitive.

Parvaresh–Vardy Codes generalize RS codes by evaluating more than just one polynomial of degree less than k at a common set of evaluation points $\mathscr{E}$.

Definition 3 (General Parvaresh–Vardy Code). Let $e(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial over $\mathbb{F}_q$ of degree $a \geq k$. Let $f_0(x) \in \mathbb{F}_q[x]_{<k}$ denote the message polynomial as for RS codes. Choose integers a, d, ℓ so that $f_i(x) \coloneqq (f_{i-1}(x))^d \mod e(x) \in \mathbb{F}_q[x]_{<k}$. A PV code of dimension k is defined as all matrices in $\mathbb{F}_q^{\ell \times n}$ such that

$$\mathrm{PV}\left[q, \mathscr{E}, k, d, \ell, e(x)\right] \coloneqq \left\{ \begin{pmatrix} \mathrm{ev}_{\mathscr{E}}(f_0) \\ \vdots \\ \mathrm{ev}_{\mathscr{E}}(f_{\ell-1}) \end{pmatrix} : \forall f_0 \in \mathbb{F}_q[x]_{<k} \right\}. \tag{2}$$

If $\ell = 1$, only the message polynomial $f_0 \in \mathbb{F}_q[x]_{<k}$ is used and PV codes (2) reduce to RS codes as in (1). For $\ell > 1$, additional algebraically correlated polynomials $f_i \in \mathbb{F}_q[x]_{<k}$ carrying no further data are evaluated for $i \in [1, \ell-1]$, so the rate of PV codes is limited to $R_{\mathrm{PV}} = k/(\ell n) = R_{\mathrm{RS}}/\ell$.

In the following, the parameters of PV codes are restricted: Let $e(x) = x^{q-1} - \alpha$ and $d = q$, such that $f_i(x) = (f_{i-1}(x))^q \mod \left(x^{q-1} - \alpha\right) = f_{i-1}(\alpha x) = f_0(\alpha^i x)$, $i \in [1, \ell-1]$, allowing for a simplified definition of PV codes:

Definition 4 (Simple Parvaresh–Vardy Code). For the choice of $\mathscr{E} = \mathbb{F}_q^*$, $e(x) = x^{q-1} - \alpha$ and $d = q$, the PV codeword symbols

$$\underline{c}_j = \left[\mathrm{ev}_{\alpha^j}(f), \mathrm{ev}_{\alpha^{j+1}}(f), \ldots, \mathrm{ev}_{\alpha^{j+\ell-1}}(f)\right]^T = \left[\mathrm{ev}_{\mathscr{E}(j,1,\ell)}(f)\right]^T \in \mathbb{F}_q^{\ell} \tag{3}$$

are based on evaluating a single polynomial $f \in \mathbb{F}_q[x]_{<k}$ at $\mathscr{E}(j, 1, \ell)$.

Note that simple PV codes use repeated evaluation points in their codewords. For example, the neighboring symbols

$$\begin{aligned} \underline{c}_j &= \left[\mathrm{ev}_{\mathscr{E}(j,1,\ell)}(f)\right]^T &&= \left[f(\alpha^j), f(\alpha^{j+1}), \ldots, f(\alpha^{j+\ell-1}) \right]^T \quad \text{and} \\ \underline{c}_{j+1} &= \left[\mathrm{ev}_{\mathscr{E}(j+1,1,\ell)}(f)\right]^T &&= \left[f(\alpha^{j+1}), \ldots, f(\alpha^{j+\ell-1}), f(\alpha^{j+\ell}) \right]^T \end{aligned}$$

have $\ell - 1$ evaluation points $\alpha^{j+1}, \ldots, \alpha^{j+\ell-1}$ in common. In general, every evaluation point is used in ℓ consecutive code symbols, therefore reducing the rate by a factor of $1/\ell$.

Folded Reed–Solomon codes avoid this rate loss by transmitting only codeword symbols at code locators $\alpha^{j\ell}$, $j \in [0, n/\ell - 1]$, eliminating repeated evaluation points. Hence, FRS codes are PV codes where symbols $\underline{c}_i$, $i \neq j\ell$, are *punctured*.

Definition 5 (Folded Reed–Solomon Code). Let the *folding parameter* $m \geq 1$ be an integer satisfying $m | n$ and α be a primitive element of $\mathbb{F}_q$. Choose $N = n/m$ disjoint ordered sets of evaluation points $\mathscr{E}(jm, 1, m) = \left\{\alpha^{jm}, \alpha^{jm+1}, \ldots, \alpha^{jm+m-1}\right\}$, $j \in [0, N-1]$. An m-FRS code of dimension k and length N consists of symbols

$$\underline{c}_j = \left[f(\alpha^{jm}), \ldots, f(\alpha^{jm+m-1})\right]^T = \left[\mathrm{ev}_{\mathscr{E}(jm,1,m)}(f)\right]^T \in \mathbb{F}_q^m. \tag{4}$$

In case $m = 1$, FRS codes reduce to RS codes. For $n = q-1$ and $\bigcup_{j=0}^{N-1} E(jm, 1, m) = \mathbb{F}_q^*$, FRS codes are essentially primitive RS codes, where m consecutive RS symbols are grouped into vectors from $\mathbb{F}_q^m$. Due to this close relationship, the rate $R_{\mathrm{FRS}} = k/n = R_{\mathrm{RS}}$ and minimum distance $d_{\min} = n - k + 1$ of FRS and RS codes are identical.

3 Decoding Radius of Linear-Algebraic MID

This section reviews linear-algebraic MID of PV, RS and FRS codes and derives a general formula for an achievable decoding radius (fraction of correctable errors) τ in terms of code and decoder parameters. The restriction to linear-algebraic algorithms allows for a much simpler presentation, but naturally leads to a slightly reduced decoding radius as well as an exponential list-size of the decoder output. The former consequence is negligible for high rate codes of practical interest and mitigation of the latter is possible [2, Sec. 4], but outside the scope of this paper.

Let $s \in [1,\ell]$ be an integer and $(s+1)$ the dimension of an interpolation point $(x, y_1, \ldots, y_s)$. Let $Q(x, y_1, \ldots, y_s) = Q_0(x) + Q_1(x)y_1 + \cdots + Q_s(x)y_s \in \mathbb{F}_q[x, y_1, \ldots, y_s]$ be an $(s+1)$-variate interpolation polynomial of degree 1 in the indeterminates $y_1, \ldots, y_s$. The codeword length shall be denoted by N and the received matrix by $\mathbf{r} = (\underline{r}_0, \underline{r}_1, \ldots, \underline{r}_{N-1}) \in \left(\mathbb{F}_q^{\ell}\right)^N$, with symbols $\underline{r}_j = [r_{j\ell}, r_{j\ell+1}, \ldots, r_{j\ell+\ell-1}]^T \in \mathbb{F}_q^{\ell}$, for $j \in [0, N-1]$. Let the $w = (1, k-1, \ldots, k-1)$-weighted degree of a monomial $x^{d_0} y_1^{d_1} \cdots y_s^{d_s}$ be defined as $\deg_w\left(x^{d_0} y_1^{d_1} \cdots y_s^{d_s}\right) \coloneqq d_0 + (k-1)\sum_{i=1}^{s} d_i$. Consequently, $\deg_w(Q)$ is the w-weighted degree of its leading monomial under w-weighted lexicographic ordering. Let $\sigma \in [1,\ell]$ denote the step size between two consecutive interpolation points within the received vector $\mathbf{r}$. Let $\mathscr{I} \subseteq [0, n-1]$ denote the set of indices $i \in \mathscr{I}$ of all $(s+1)$-dimensional interpolation points $(\alpha^i, r_{\sigma i}, \ldots, r_{\sigma i+s-1})$ used by the decoding algorithm and let $I \coloneqq |\mathscr{I}|$ be its cardinality.

Linear-algebraic MID consists of an interpolation step and a root-finding step: In the **interpolation step,** the decoder finds a nonzero $(s+1)$-variate polynomial $Q \in \mathbb{F}_q[x, y_1, \ldots, y_s]$ of minimal $\deg_w(Q) = D$ and degree 1 in $y_1, \ldots, y_s$, satisfying

$$Q(\alpha^i, r_{\sigma i}, \ldots, r_{\sigma i+s-1}) = 0, \quad \forall i \in \mathscr{I}, \tag{5}$$

giving a total of I constraints on at most $(s+1)(D+1) - s(k-1)$ coefficients of Q. If D is large enough, the resulting homogeneous linear system of (5) has a nonzero solution for Q. The minimal such w-weighted degree is given in terms of I and s as

$$D(I,s) \coloneqq \left\lfloor \frac{I + s(k-1)}{s+1} \right\rfloor. \tag{6}$$

In the **root-finding step** a list of candidate message polynomials $f \in \mathbb{F}_q[x]_{<k}$ is recovered from $\mathbf{r}$. For the codes and algorithms considered in this paper, it suffices to find all y-roots $f_0 \in \mathbb{F}_q[x]_{<k}$ of Q, such that f_i, $i \in [0, s-1]$, satisfies

$$Q(x, f_0(x), f_1(x), \ldots, f_{s-1}(x)) = 0. \tag{7}$$

Denote by $E \coloneqq \left|\left\{ j \in [0, N-1] : \underline{r}_j \neq \underline{c}_j \right\}\right|$ the total number of received symbols in error. An interpolation point $(\alpha^i, r_{\sigma i}, \ldots, r_{\sigma i+s-1})$, $i \in \mathscr{I}$, is said to agree with a message polynomial $f_0 \in \mathbb{F}_q[x]_{<k}$ if $r_t = f_{t \mod \ell}(\alpha^i)$, $t \in [\sigma i, \sigma i + s - 1]$.

Lemma 1. *The maximum number of interpolation points corrupted by a single received symbol error $\underline{r}_j \neq \underline{c}_j$, $j \in [0, N-1]$, is given by*

$$A(\mathscr{I}, \ell, s, \sigma) \coloneqq \max_j \left|\left\{ i \in \mathscr{I} : [\sigma i, \sigma i + s - 1] \cap [j\ell, j\ell + \ell - 1] \neq \emptyset \right\}\right|. \tag{8}$$

Proof: An $(s+1)$-dimensional interpolation point $(\alpha^i, r_{\sigma i}, \ldots, r_{\sigma i+s-1})$, $i \in \mathscr{I}$, corresponds to indices $[\sigma i, \sigma i+s-1]$ in the received vector $\mathbf{r}$. A received symbol $\underline{r}_j \in \mathbb{F}_q^\ell$ uses indices $[j\ell, j\ell+\ell-1]$. The j-th symbol $\underline{r}_j$ affects the i-th interpolation point if and only if the intersection $[\sigma i, \sigma i+s-1] \cap [j\ell, j\ell+\ell-1]$ is not empty. ■

Lemma 2. *An $(s+1)$-variate polynomial $Q \in \mathbb{F}_q[x, y_1, \ldots, y_s]$ of $\deg_w(Q) = D(I,s)$ satisfying (5) will satisfy (7) if the number of agreements $I - EA(\mathscr{I}, \ell, s, \boldsymbol{\sigma}) > D(I,s)$.*

Proof: According to the *Polynomial Factor Theorem* [7, Cor. X.1.4], the number of roots of a non-constant univariate polynomial $P(x) = Q(x, f_0(x), \ldots, f_{s-1}(x)) \in \mathbb{F}_q[x]_{\leq D(I,s)}$ cannot exceed its degree, implying $Q(x, f_0(x), f_1(x), \ldots, f_{s-1}(x)) \equiv 0$. ■

Theorem 1. *In case (7) suffices to recover all candidate polynomials $f_0 \in \mathbb{F}_q[x]_{<k}$, a fraction of correctable errors τ is achievable if*

$$\tau \leq \left(\frac{s}{s+1}\right)\left(\frac{I-k}{A(\mathscr{I}, \ell, s, \boldsymbol{\sigma})N}\right). \tag{9}$$

Proof: Combining (6) and Lemma 2, we can choose any

$$\tau \leq \frac{E}{N} < \frac{1}{A(\mathscr{I}, \ell, s, \boldsymbol{\sigma})N}\left\lceil \frac{s(I-k)+1}{s+1} \right\rceil.$$

■

The result of Theorem 1 is applied to the following codes and decoding algorithms:

1) Decoding of RS Codes (BW Algorithm): RS codes use $\ell = 1$ message polynomial, $N = n$ symbols $\underline{c}_j \in \mathbb{F}_q$ and $\boldsymbol{\sigma} = 1$. The decoder finds a bivariate polynomial $Q(x,y) = Q_0(x) + Q_1(x)y \in \mathbb{F}_q[x,y]$ of minimal $w = (1, k-1)$-weighted degree, passing through all $(s+1) = 2$-dimensional points (α^i, r_i), $i \in \mathscr{I} = [0, n-1]$. Due to (6), $\deg_w(Q) \geq D(n,1) = \left\lfloor \frac{n+k-1}{2} \right\rfloor$ is needed to satisfy all $I = n$ conditions. A symbol error affects $A(\mathscr{I}, 1, 1, 1) = 1$ interpolation point. Theorem 1 guarantees a fraction of correctable errors

$$\tau_{\mathrm{BW}} = (1-R)/2 \tag{10}$$

up to which the message polynomial $f \in \mathbb{F}_q[x]_{<k}$ can be recovered [6, Thm. 5.2.2].

2) Decoding of PV Codes: A rate R_{PV} PV code uses $N = n$ symbols $\underline{c}_j \in \mathbb{F}_q^\ell$. An $(\ell+1)$-variate polynomial $Q(x, y_1, \ldots, y_\ell) = Q_0(x) + Q_1(x)y_1 + \cdots + Q_\ell(x)y_\ell \in \mathbb{F}_q[x, y_1, \ldots, y_\ell]$ of $w = (1, k-1, \ldots, k-1)$-weighted degree is found, passing through $(\ell+1)$-dimensional interpolation points $(\alpha^i, r_{i\ell}, \ldots, r_{i\ell+\ell-1})$, for $i \in \mathscr{I} = [0, n-1]$. Hence, $I = n$ and $\deg_w(Q) \geq D(n, \ell) = \left\lfloor \frac{n+\ell(k-1)}{\ell+1} \right\rfloor$. In case $\underline{r}_j \neq \underline{c}_j$, $A(\mathscr{I}, \ell, \ell, \ell) = 1$ due to $\boldsymbol{\sigma} = \ell$. Theorem 1 states that an achievable fraction of correctable errors is

$$\tau_{\mathrm{PV}} = \ell/(\ell+1)(1 - \ell R_{\mathrm{PV}}) \tag{11}$$

such that a list of message polynomials $f_0 \in \mathbb{F}_q[x]_{<k}$ can be recovered [8, Lem. 6–9].

3) FRS Decoding Scheme A: FRS codes are punctured PV codes with $\ell = m$, $\boldsymbol{\sigma} = 1$, symbols $\underline{c}_j \in \mathbb{F}_q^m$ and $N = n/m$. In the linear-algebraic decoding scheme by Vadhan [10, 5], $\mathscr{I}$ is chosen so that all points $(\alpha^i, r_i, \ldots, r_{i+s-1})$ are strictly contained inside the received symbols, i.e., $i \in \bigcup_{j=0}^{N-1}[mj, mj+m-1]$. Therefore, $I = N(m-s+1)$ and $A(\mathscr{I}, m, s, 1) = m-s+1$. An $(s+1)$-variate polynomial $Q \in \mathbb{F}_q[x, y_1, \ldots, y_s]$ is found if $\deg_w(Q) \geq D(N(m-s+1), s) = \left\lfloor \frac{N(m-s+1)+s(k-1)}{s+1} \right\rfloor$.

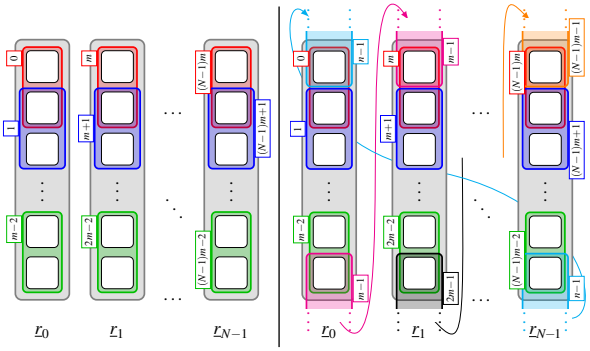

Fig. 1 FRS decoding schemes A (left) and B (right) using 3-variate interpolation. White boxes represent symbols from $\mathbb{F}_q$, grouped into interpolation points with code locator exponent in square boxes. Gray boxes denote received symbols $\underline{r}_j \in \mathbb{F}_q^m$, $j \in [0, N-1]$. Dotted borders with arrows depict overlapping interpolation points between neighboring symbols.

Due to [5, Lem. 6] and (9), we can achieve a fraction of correctable errors

$$\tau_{\mathrm{FRS_A}} = \frac{s}{s+1}\left(1 - \left(\frac{m}{m-s+1}\right)R\right) \qquad \text{for } 0 \le R \le (m-s+1)/m. \tag{12}$$

4) FRS Decoding Scheme B: Another scheme suggested by Justesen [2, Sec. 3.2] uses all $I = n$ interpolation points, thus requiring $\deg_w(Q) \ge D(n,s) = \left\lfloor \frac{n+s(k-1)}{s+1} \right\rfloor$. Due to the FRS code design, the cost of increasing I is that interpolation points overlap into neighboring code symbols. A symbol error affects $A(\mathscr{I}, m, s, 1) = m+s-1$, i.e., an extra $2(s-1)$ points over Scheme A. An achievable decoding radius is

$$\tau_{\mathrm{FRS_B}} = \frac{s}{s+1}\left(\frac{m}{m+s-1}\right)(1-R) \qquad \text{for } 0 \le R \le 1. \tag{13}$$

Note that $\tau_{\mathrm{FRS_B}} > \tau_{\mathrm{FRS_A}}$ if $R > (m-s+1)/(2m)$.

4 Optimal Design of FRS Codes in Terms of Decoding Radius

According to Theorem 1, τ is a function of the interpolation parameter $s \in [1, m]$, the number of interpolation points $I \in [1, n]$ used, code length $N = n/m$ and maximum number of interpolation points $A(\mathscr{I}, m, s, \boldsymbol{\sigma}) \in [I/N, m+s-1]$ affected by one symbol error. The range of parameters s and I is straightforward. The minimum value of $A(\mathscr{I}, m, s, \boldsymbol{\sigma})$ results from uniformly distributing I interpolation points among N code symbols. The maximum results from the maximum number of distinct $(s+1)$-dimensional points touching a symbol from $\mathbb{F}_q^m$. In order to maximize the decoding radius in (9), the optimal parameters are $s_{\mathrm{opt}} = m$, $I_{\mathrm{opt}} = n$ and $A_{\mathrm{opt}} = m$, such that

$$\tau_{\mathrm{opt}} = m/(m+1)(1-R). \tag{14}$$

Neither FRS decoding scheme A (using only $I = N(m-s+1) < I_{\mathrm{opt}}$ interpolation points) nor scheme B (with $A(\mathscr{I}, m, s, 1) = m+s-1 > A_{\mathrm{opt}}$ interpolation points affected by a symbol error) use these optimal values. In order to achieve the optimal parameters $I_{\mathrm{opt}} = n$ and $A_{\mathrm{opt}} = m$, FRS codes shall be adapted as follows: Based on FRS scheme B, the $2(s-1)$ transboundary $(s+1)$-dimensional interpolation points shall "wrap around" into the *same* code symbol instead of a neighboring one. This

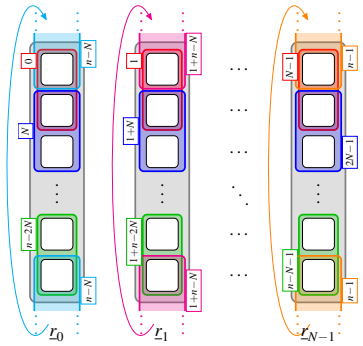

Fig. 2 MID of m-LOFRS code using 3-dimensional interpolation points. Dotted boxes with arrows depict interpolation points wrapping around into the *same* codeword symbol.

prevents crosstalk of erroneous interpolation points between neighboring symbols in case of symbol errors. The rate increase of an $\ell = m$-FRS over an ℓ-order PV code is due to the use of disjoint evaluation sets in (4), which shall be retained.

Definition 6 (Low-Order FRS Code). Let the *folding parameter* $m \geq 1$ be such that $m|n$ for $n = q-1$ and let α be a primitive element of $\mathbb{F}_q$. Choose $N = {}^{n}/_{m}$ disjoint sets of evaluation points $\mathscr{E}(j,N,m) = \{\alpha^j, \alpha^{j+N}, \alpha^{j+2N}, \ldots, \alpha^{j+n-N}\}, j \in [0,N-1]$ such that $\bigcup_{j=0}^{N-1} \mathscr{E}(j,N,m) = \mathbb{F}_q^*$. Note that α^N is an element of low order. A *low-order* m-FRS (LOFRS) code of dimension k and length N consists of symbols

$$\underline{c}_j = \left[f(\alpha^j), f(\alpha^{j+N}), \ldots, f(\alpha^{j+n-N})\right]^T = \left[\mathrm{ev}_{\mathscr{E}(j,N,m)}(f)\right]^T \in \mathbb{F}_q^m. \tag{15}$$

For $m = 1$, LOFRS codes reduce to RS codes.

As for regular m-FRS codes, the decoder finds an $(s+1)$-variate interpolation polynomial $Q \in \mathbb{F}_q[x, y_1, \ldots, y_s]$ passing through all $I = n$ interpolation points, i.e., satisfying (5) for $i \in \mathscr{I} = \bigcup_{j=0}^{N-1}\{j + N[0, m-1]\}$. Using (6), a $w = (1, k-1, .., k-1)$-weighted degree $\deg_w(Q) \geq D(n,s) = \left\lfloor \frac{n+s(k-1)}{s+1} \right\rfloor$ is required. Due to the choice of $\mathscr{I}$ and $\sigma = 1$, inter-symbol crosstalk of interpolation points is avoided in case of $\underline{r}_j \neq \underline{c}_j$ and so $A(\mathscr{I}, m, s, 1) = m = A_{\text{opt}}$, see Figure 2 for $(s+1) = 3$. In the root-finding step, a list of message polynomials $f \in \mathbb{F}_q[x]_{<k}$ is recovered [4, Prop. 5.3] from $Q(x, f(x), f(\alpha^N x), \ldots, f(\alpha^{(s-1)N})) = 0$ if the agreement between $\mathbf{r}$ and f is larger than $D(n,s)$. Hence, it is possible to achieve a fraction of correctable errors

$$\tau_{\text{LOFRS}} = s/(s+1)(1-R) > \max\{\tau_{\text{FRS}_\text{A}}, \tau_{\text{FRS}_\text{B}}\} \qquad \text{for } 0 \leq R \leq 1. \tag{16}$$

By choosing the maximum interpolation parameter $s_{\text{opt}} = m$, the optimal decoding radius $\tau_{\text{LOFRS}} = \tau_{\text{opt}}$ is reached. In contrast, for FRS schemes A and B we have

$$\tau_{\text{FRS}_\text{A}} = m/(m+1)(1-mR) \qquad = \tau_{\text{PV}} \tag{17}$$

$$\tau_{\text{FRS}_\text{B}} = m/(m+1)(m)/(2m-1)(1-R) \approx \tau_{\text{BW}}. \tag{18}$$

Figure 3 compares the decoding radius of the BW algorithm for RS codes (10), linear-algebraic decoding of order $\ell = 5$ PV codes (11), $m = 5$-FRS decoding scheme A (12), decoding scheme B (13) and $m = 5$-LOFRS codes (16) for $s \in [2, m]$.

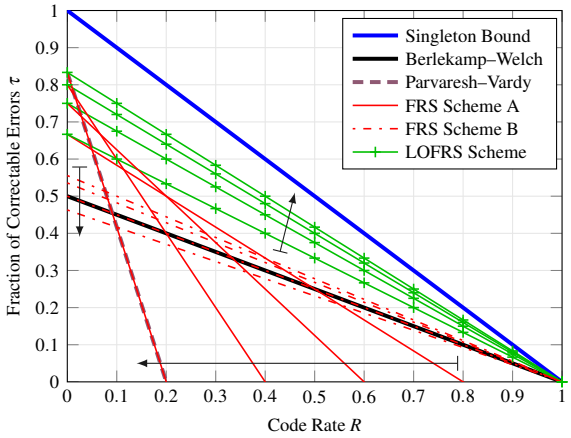

Fig. 3 Linear-algebraic MID radius τ versus code rate R of $\ell = 5$ PV codes, $m = 5$-FRS decoding schemes A and B, and proposed $m = 5$-LOFRS codes for parameter $s \in [2, m]$ (increasing along arrows).

5 Conclusion

A general formula for the error-correcting radius of linear-algebraic MID of RS, PV and FRS codes was derived and analyzed. Through this formula, an improved design of m-FRS codes called *Low-Order m-FRS* codes was motivated, which was recently introduced by [4]. The proposed codes can be viewed in the context of punctured PV codes and they reach the optimal decoding radius $\tau_{\text{opt}} = m/(m+1)(1-R)$.

Acknowledgements The author is supported by the German Ministry of Education and Research in the framework of the Alexander von Humboldt-Professorship and thanks G. Kramer, F. Kschischang, and V. Sidorenko as well as C. Senger, H. Bartz for their comments and discussions.

References

1. Gemmell, P., Sudan, M.: Highly resilient correctors for polynomials. Inform. Process. Lett. **43**(4), 169–174 (1992)
2. Guruswami, V., Rudra, A.: Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy. IEEE Trans. Inf. Theory **54**(1), 135–150 (2008)
3. Guruswami, V., Sudan, M.: Improved decoding of Reed–Solomon and algebraic-geometry codes. IEEE Trans. Inf. Theory **45**(6), 1757–1767 (1999)
4. Guruswami, V., Wang, C.: Explicit rank-metric codes list-decodable with optimal redundancy. CoRR **abs/1311.7084** (2013)
5. Guruswami, V., Wang, C.: Linear-algebraic list decoding for variants of Reed–Solomon codes. IEEE Trans. Inf. Theory **59**(6), 3257–3268 (2013)
6. Justesen, J., Høholdt, T.: A Course in Error-Correcting Codes. Eur. Math. Soc., Zürich (2004)
7. Lang, S.: Algebra, *Grad. Texts in Math.*, vol. 211. Springer-Verlag, New York, 3rd edn. (2002)
8. Parvaresh, F., Vardy, A.: Correcting errors beyond the Guruswami–Sudan radius in polynomial time. In: Proc. 46th IEEE Symp. on Found. Comp. Science, pp. 285–294 (2005)
9. Sudan, M.: Decoding of Reed–Solomon codes beyond the error-correction bound. J. Complexity **13**(1), 180–193 (1997)
10. Vadhan, S.: Pseudorandomness. Found. Trends Theor. Comput. Sci. (2011)
11. Welch, L., Berlekamp, E.: Error correction for algebraic block codes. US Pat. 4,633,470 (1986)