Des. Codes Cryptogr. (2017) 82:449–467
DOI 10.1007/s10623-016-0195-6

Algebraic decoding of folded Gabidulin codes

Hannes Bartz[1] · **Vladimir Sidorenko**[1,2]

Received: 12 October 2015 / Accepted: 2 March 2016 / Published online: 23 March 2016

Abstract An efficient interpolation-based decoding algorithm for h-folded Gabidulin codes is presented that can correct rank errors beyond half the minimum rank distance for any code rate $0 \leq R \leq 1$. The algorithm serves as a list decoder or as a probabilistic unique decoder and improves upon existing schemes, especially for high code rates. A probabilistic unique decoder with adjustable decoding radius is presented. The decoder outputs a unique solution with high probability and requires at most $\mathcal{O}(s^2n^2)$ operations in $\mathbb{F}_{q^m}$, where $1 \leq s \leq h$ is a decoding parameter and $n \leq m$ is the length of the unfolded code over $\mathbb{F}_{q^m}$. An upper bound on the average list size of folded Gabidulin codes and on the decoding failure probability of the decoder is given. Applying the ideas to a list decoding algorithm by Mahdavifar and Vardy (List-decoding of subspace codes and rank-metric codes up to Singleton bound, ISIT 2012) improves the performance when used as probabilistic unique decoder and gives an upper bound on the failure probability.

Keywords Rank-metric codes · Folded Gabidulin codes · Probabilistic unique decoding · Interpolation-based decoding

Mathematics Subject Classification Primary 94B35 · 94B05

This is one of several papers published in *Designs, Codes and Cryptography* comprising the "Special Issue on Coding and Cryptography".

✉ Hannes Bartz
hannes.bartz@tum.de

Vladimir Sidorenko
vladimir.sidorenko@tum.de

[1] Institute for Communications Engineering, Technical University of Munich, 80290 Munich, Germany

[2] Institute for Information Transmission Problems, Russian Academy of Science, Moscow, Russia

1 Introduction

Decoding schemes for folded Gabidulin codes were independently introduced in [13] and [10]. Both constructions allow to correct rank errors up to the Singleton bound in rank-metric for very small code rates.

We present a new interpolation-based decoding algorithm for folded Gabidulin codes that can correct rank errors beyond half the minimum rank distance for any code rate. This scheme can be used as a list decoder which outputs a list of all codewords up to the decoding radius. Although the worst-case list size of this approach is exponential in the length of the code, we show that the decoder returns a list of size one with high probability. This allows to use the scheme as a probabilistic unique decoder that outputs a unique solution by allowing a very low failure probability. We present a probabilistic unique decoding algorithm with adjustable decoding radius that allows to further reduce the failure probability by backing off the decoding radius.

We compare our results for folded Gabidulin codes with punctured (or interleaved) Gabidulin codes. Punctured Gabidulin codes with probabilistic unique decoding were proposed in [12,16] and [19]. These decoding algorithms achieve the best known decoding radius close to the Singleton bound by allowing decoding failures with small probability. Later in [9] a list decoding algorithm for punctured Gabidulin codes was suggested, which has the same decoding radius when the list size is allowed to be exponential in the code length. An explicit construction and a list decoding algorithm for punctured Gabidulin codes was presented in [8]. The output of this decoder is a basis for the affine subspace containing all candidate messages, which is a large list with high probability.

This paper is structured as follows. In Sect. 2, we describe the notation and give basic definitions. Section 3 explains the ideas of our interpolation-based decoding algorithm for folded Gabidulin codes and shows the improvements upon existing schemes for high code rates. In Sect. 4, we show how the interpolation-based decoder can be used for list and probabilistic unique decoding of folded Gabidulin codes. Section 5 describes how these results apply to the decoding scheme by Mahdavifar and Vardy [13]. Section 6 concludes this paper.

Part of this work was presented at the International Workshop on Coding and Cryptography (WCC), Apr. 2015, Paris, France [1]. In this paper we give detailed proofs and extend the results to probabilistic unique decoding of low-rate folded Gabidulin codes.

2 Preliminaries

2.1 Finite fields and matrices

Let q be a power of a prime, denote by $\mathbb{F}_q$ the finite field of order q and by $\mathbb{F}_{q^m}$ its extension field of degree m. Vectors and matrices are denoted by bold lowercase and uppercase letters such as $\mathbf{a}$ and $\mathbf{A}$ and their elements are indexed beginning from zero. We denote the rank and the kernel of a matrix $\mathbf{A} \in \mathbb{F}_q^{m\times n}$ over $\mathbb{F}_q$ by $\mathrm{rk}(\mathbf{A})$ and $\ker(\mathbf{A})$, respectively. There is a bijective mapping between any row vector $\mathbf{a} \in \mathbb{F}_{q^m}^n$ and a matrix $\mathbf{A} \in \mathbb{F}_q^{m\times n}$ under any fixed basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. The rank of a row vector $\mathbf{a} \in \mathbb{F}_{q^m}^n$ is defined as $\mathrm{rk}(\mathbf{a}) = \mathrm{rk}(\mathbf{A})$ where $\mathbf{A} \in \mathbb{F}_q^{m\times n}$ is the corresponding matrix over $\mathbb{F}_q$. By $[a, b]$ we denote the set of integers $\{a, a+1, \ldots, b\}$.

2.2 Linearized polynomials

For any element $\alpha \in \mathbb{F}_{q^m}$ and any integer i let $\alpha^{[i]} \stackrel{\text{def}}{=} \alpha^{q^i}$ be the Frobenius power of α. A nonzero polynomial of the form

$$p(x) = \sum_{i=0}^{l} p_i x^{[i]} \tag{1}$$

with $p_i \in \mathbb{F}_{q^m}$, $p_l \neq 0$, is called a *linearized polynomial* of q-degree $\deg_q(p(x)) = l$, see [11,15]. The set of all roots of $p(x)$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}$. A linearized polynomial of q-degree l can have at most l linearly independent roots in $\mathbb{F}_{q^m}$, i.e., a root space of dimension at most l. If the dimension of the root space of a linearized polynomial $p(x)$ equals the q-degree $\deg_q(p(x))$ we call it a *minimal linearized polynomial* for this root space. The evaluation of a linearized polynomial forms a linear map over $\mathbb{F}_q$, i.e., for all $a, b \in \mathbb{F}_q$ and $x_1, x_2 \in \mathbb{F}_{q^m}$, we have

$$p(ax_1 + bx_2) = ap(x_1) + bp(x_2). \tag{2}$$

The noncommutative composition

$$p^{(1)}(x) \otimes p^{(2)}(x) \stackrel{\text{def}}{=} p^{(1)}(p^{(2)}(x))$$

of two linearized polynomials $p^{(1)}(x)$ and $p^{(2)}(x)$ of q-degree d_1 and d_2 is a linearized polynomial of q-degree $d_1 + d_2$. The set of all linearized polynomials over $\mathbb{F}_{q^m}$ forms a noncommutative ring $\mathbb{L}_{q^m}[x]$ with identity under addition "+" and composition "$\otimes$". We denote the set of all linearized polynomials from $\mathbb{L}_{q^m}[x]$ with q-degree less than k by $\mathbb{L}_{q^m}[x]_{<k}$.

Lemma 1 *The set $\mathbb{L}_{q^m}[x]_{<k}$ forms a commutative group under addition "+".*

Proof The coefficients of every linearized polynomial of degree at most $k-1$ can be written as a vector of length k over $\mathbb{F}_{q^m}$. The addition of polynomials is equivalent to the addition of the coefficient vectors over the field and the statement of the lemma follows. □

The *Moore* matrix of a vector $\mathbf{a} = (a_0\ a_1\ \ldots\ a_{n-1}) \in \mathbb{F}_{q^m}^n$ is defined as

$$\mathbf{M}_r(\mathbf{a}) = \begin{pmatrix} a_0 & a_1 & \ldots & a_{n-1} \\ a_0^{[1]} & a_1^{[1]} & \ldots & a_{n-1}^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ a_0^{[r-1]} & a_1^{[r-1]} & \ldots & a_{n-1}^{[r-1]} \end{pmatrix}. \tag{3}$$

The rank of $\mathbf{M}_r(\mathbf{a})$ is $\min\{r, n\}$ if the elements $a_0, \ldots, a_{n-1}$ are linearly independent over $\mathbb{F}_q$, see [11].

2.3 (Folded) Gabidulin codes

A rank-metric code $\mathcal{C}$ of length N is a set of $M \times N$ matrices over $\mathbb{F}_q$. Each codeword of $\mathcal{C}$ can be represented by a vector of length N over $\mathbb{F}_{q^M}$. The minimum rank distance d of $\mathcal{C}$ is defined as

$$d = \min_{\mathbf{x},\mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}} d_r(\mathbf{x}, \mathbf{y}) \stackrel{\text{def}}{=} \min_{\mathbf{x},\mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}} \mathrm{rk}(\mathbf{X} - \mathbf{Y}) \tag{4}$$

where $\mathbf{X}, \mathbf{Y}$ are the matrix representations of $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ over $\mathbb{F}_q$. If $\mathcal{C}$ forms a group under addition over $\mathbb{F}_q$ we have $\mathbf{X}' = \mathbf{X} - \mathbf{Y} \in \mathcal{C} \setminus \{\mathbf{0}\}$ for $\mathbf{X} \neq \mathbf{Y}$ and get

$$d = \min_{\mathbf{x},\mathbf{y}\in\mathcal{C},\mathbf{x}\neq\mathbf{y}} \operatorname{rk}(\mathbf{X} - \mathbf{Y}) = \min_{\mathbf{x}'\in\mathcal{C}\setminus\{\mathbf{0}\}} \operatorname{rk}(\mathbf{X}').$$

In this case the minimum distance corresponds to the minimum rank of a nonzero codeword in $\mathcal{C}$.

Denote by $\mathcal{B}^{(t)}(\mathbf{Y})$ a ball of radius t in rank-metric around a matrix $\mathbf{Y}$ containing all matrices lying within rank distance at most t from $\mathbf{Y}$. The volume $|\mathcal{B}^{(t)}(\mathbf{Y})|$ is independent of the center $\mathbf{Y}$ (see e.g., [6]).

The Singleton-like bound for rank-metric codes states that

$$\begin{aligned} |\mathcal{C}| &\leq \left(q^M\right)^{N-d+1} \\ \iff \quad d &\leq N - \log_{q^M}(|\mathcal{C}|) + 1. \end{aligned} \tag{5}$$

if $M \geq N$, see [4,5].

Codes which fulfill this bound with equality are called *maximum rank distance* (MRD) codes. A special class of MRD codes are *Gabidulin codes* [4,5], which are the analogs of Reed–Solomon codes in rank-metric. As channel model we use the rank error channel

$$\mathbf{Y} = \mathbf{C} + \mathbf{E}. \tag{6}$$

For fixed $t = \operatorname{rk}(\mathbf{E})$ the error matrix $\mathbf{E}$ is assumed to be uniformly distributed over all $M \times N$ matrices of rank t over $\mathbb{F}_q$.

Folded Gabidulin codes were proposed independently in [13] and [10]. In [10] the coefficients of the message polynomial are restricted to belong to a subfield of $\mathbb{F}_{q^m}$. In this work we consider folded Gabidulin codes as defined in [13].

Definition 1 *(h-folded Gabidulin code)* Let $\{\alpha^0, \alpha^1, \ldots, \alpha^{n-1}\} \subset \mathbb{F}_{q^m}$ with $n \leq m$ be linearly independent over $\mathbb{F}_q$ called code locators. Let h be a positive integer that divides n and let $N = n/h$. An h-folded Gabidulin code FGab$[h; n, k]$ of length N, dimension k is defined as

$$\left\{ \left(\begin{bmatrix} f(\alpha^0) \\ f(\alpha^1) \\ \vdots \\ f(\alpha^{h-1}) \end{bmatrix}, \begin{bmatrix} f(\alpha^h) \\ f(\alpha^{h+1}) \\ \vdots \\ f(\alpha^{2h-1}) \end{bmatrix}, \ldots, \begin{bmatrix} f(\alpha^{n-h}) \\ f(\alpha^{n-h+1}) \\ \vdots \\ f(\alpha^{n-1}) \end{bmatrix} \right) : f(x) \in \mathbb{L}_{q^m}[x]_{<k} \right\}. \tag{7}$$

A codeword of an h-folded Gabidulin code is a matrix $\mathbf{c} \in \mathbb{F}_{q^m}^{h\times N}$ or $\mathbf{C} \in \mathbb{F}_q^{hm\times N}$ where each element of $\mathbb{F}_{q^m}$ is written as a column vector of length m over $\mathbb{F}_q$. The jth column of $\mathbf{c}$ is

$$\mathbf{c}_j = \left(f(\alpha^{jh}) \ldots f(\alpha^{(j+1)h-1}) \right)^T$$

and can be seen as an element of the field $\mathbb{F}_{q^{hm}}$ for $j \in [0, N-1]$. Folded Gabidulin codes are codes of length N over a large field $\mathbb{F}_{q^M} = \mathbb{F}_{q^{hm}}$ that can be decoded over the small field $\mathbb{F}_{q^m}$. An h-folded Gabidulin code is a *nonlinear* code over $\mathbb{F}_{q^{hm}}$ since for any $a, b \in \mathbb{F}_{q^{hm}}$ and any $\mathbf{c}, \mathbf{c}' \in \mathcal{C}$ the $\mathbb{F}_{q^{hm}}$-linear combination $a\mathbf{c} + b\mathbf{c}'$ is not necessarily contained in $\mathcal{C}$. A folded Gabidulin code is $\mathbb{F}_{q^m}$-linear since the unfolded code is an $\mathbb{F}_{q^m}$-linear subspace of $\mathbb{F}_{q^m}^n$. This also implies that the code is *linear* over $\mathbb{F}_q$.

The number of codewords in $\mathcal{C}$ is $|\mathcal{C}| = q^{mk}$. The code rate of a folded Gabidulin code is the same as the code rate of the unfolded code [13], i.e.,

$$R = \frac{\log_{q^{hm}}(|\mathcal{C}|)}{N} = \frac{k}{n}.$$

The following theorem shows that folded Gabidulin codes are MRD codes if and only if h divides k.

Theorem 1 *The minimum rank distance of an h-folded Gabidulin code $\mathcal{C}$ with parameters $n, k, h, N = \frac{n}{h}$ is $d = N - \lceil \frac{k}{h} \rceil + 1$.*

Proof An h-folded Gabidulin code forms a group under addition since $\mathbb{L}_{q^m}[x]_{<k}$ forms an additive group over $\mathbb{F}_{q^m}$ by Lemma 1. Thus the minimum distance of the code is given by the minimum rank of a nonzero codeword, i.e.,

$$d = \min_{\mathbf{c} \in \mathcal{C}^*} \mathrm{rk}(\mathbf{C})$$

where $\mathcal{C}^* \stackrel{\text{def}}{=} \mathcal{C} \setminus \{\mathbf{0}\}$. Let $\mathbf{C} \in \mathcal{C}^*$ be a codeword generated by the evaluation of $f(x) \in \mathbb{L}_{q^m}[x]_{<k}$ at the code locators $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$. Since $N \leq hm$ we have $\mathrm{rk}(\mathbf{C}) \leq N$. If the column rank of $\mathbf{C}$ is

$$\mathrm{rk}(\mathbf{C}) = N - z$$

then by $\mathbb{F}_q$-elementary column operations (Gaussian elimination) we will get $\mathbf{C}'$ with z zero columns and $N - z$ linearly independent columns. From (2) it follows that $\mathbf{C}'$ is generated by the evaluation of $f(x)$ at the new code locators α_i' that are obtained from α_i by $\mathbb{F}_q$-elementary operations for all $i \in [0, n-1]$. Thus the new code locators $\{\alpha_0', \alpha_1' \ldots, \alpha_{n-1}'\}$ are linearly independent and we have $f(\alpha_i') = 0$ for all $i \in [0, n-1]$ at most $k-1$ times. Hence the number of zero columns z in $\mathbf{C}'$ satisfies

$$z \leq \left\lfloor \frac{k-1}{h} \right\rfloor = \left\lceil \frac{k}{h} \right\rceil - 1 \tag{8}$$

and

$$d = \min_{\mathbf{c} \in \mathcal{C}^*} \mathrm{rk}(\mathbf{C}) \geq N - \left\lceil \frac{k}{h} \right\rceil + 1. \tag{9}$$

From the Singleton bound (5) we have

$$\begin{aligned} &\log_{q^{hm}} q^{mk} \leq N - d + 1 \\ \iff \quad &d \leq N - \frac{k}{h} + 1. \end{aligned} \tag{10}$$

Combining (9) and (10) we get

$$N - \left\lceil \frac{k}{h} \right\rceil + 1 \leq d \leq N - \frac{k}{h} + 1 \tag{11}$$

and the statement of the theorem follows, since d is an integer. □

Thus folded Gabidulin codes fulfill the Singleton bound (5) with equality (i.e., are MRD codes) if and only if h divides k. If h does *not* divide k then the code has still the best minimum distance for the given parameters N, k and h but the size of the code book could be larger in this case.

3 Improved interpolation-based decoding of high-rate folded Gabidulin codes

The interpolation-based list decoding algorithm for folded Gabidulin codes by Mahdavifar and Vardy in [13] is closely related to the list decoding algorithm for folded Reed–Solomon codes by Guruswami and Rudra [7] and Vadhan [17]. The normalized decoding radius $\tau_{\mathrm{MV}} = t/N$ of this decoder is

$$\tau_{\mathrm{MV}} < \frac{s}{s+1}\left(1 - \frac{h}{h-s+1}R\right) \tag{12}$$

where the integer $1 \le s \le h$ is a decoding parameter. For $s \approx \sqrt{h}$ a normalized decoding radius $\tau_{\mathrm{MV}} < 1 - R - \epsilon$ with $\epsilon = 1/2s$ can be achieved (see [13, Theorem 12]). Observe that τ_{MV} is positive if $R < \frac{h-s+1}{h}$. Thus the decoder in [13] cannot correct any errors for code rates larger than $\frac{h-s+1}{h}$ (or $1 - \frac{\sqrt{h}-1}{h}$ for $s = \sqrt{h}$). But many applications require high-rate codes.

In this section we present an improved list decoding scheme that can correct errors beyond the unique decoding radius $d/2$ for any code rate $R > 0$. The scheme is motivated by Justesen's idea for decoding folded Reed–Solomon codes [7, Sec. III-B] and improves upon [13] for high code rates.

Our decoding scheme consists of an interpolation step and a root-finding step. In comparison with [13] the code construction remains the same (Definition 1) but the set of interpolation points in the interpolation step is chosen differently.

3.1 Interpolation step

Suppose we receive a matrix

$$\mathbf{y} = \left(\begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{h-1} \end{bmatrix}, \begin{bmatrix} y_h \\ y_{h+1} \\ \vdots \\ y_{2h-1} \end{bmatrix}, \ldots, \begin{bmatrix} y_{n-h} \\ y_{n-h+1} \\ \vdots \\ y_{n-1} \end{bmatrix} \right) = \mathbf{c} + \mathbf{e} \tag{13}$$

where $\mathbf{e} = \left(\mathbf{e}_0^T, \mathbf{e}_1^T, \ldots, \mathbf{e}_{N-1}^T\right) \in \mathbb{F}_{q^m}^{h \times N}$ with row vectors $\mathbf{e}_j \in \mathbb{F}_{q^m}^h$. The error matrix over $\mathbb{F}_q$ is denoted by $\mathbf{E} = \left(\mathbf{E}_0^T, \mathbf{E}_1^T, \ldots, \mathbf{E}_{N-1}^T\right) \in \mathbb{F}_q^{hm \times N}$ with $\mathbf{E}_j \in \mathbb{F}_q^{hm}$. Denote by

$$\mathbf{y}_j = (y_{jh}\ y_{jh+1} \cdots y_{(j+1)h-1})^T \in \mathbb{F}_{q^m}^h$$

the jth column of $\mathbf{y}$ for $j \in [0, N-1]$. The code locators in Definition 1 are consecutive powers of a primitive element $\alpha \in \mathbb{F}_{q^m}$ and thus form a *polynomial basis* over $\mathbb{F}_q$. This allows to use $(s+1)$-dimensional interpolation points of the form

$$\left(\alpha^i, y_i, y_{i+1}, \ldots, y_{i+s-1}\right), \qquad i \in [0, n-s].$$

In other words, the received symbols $\mathbf{y}_j$ of the received matrix $\mathbf{y}$ in (13) are sampled using a sliding window of size s. The choice of the interpolation points is crucial for the performance of the decoder.

In [13] each $(s+1)$-dimensional interpolation point only contains values strictly chosen from one received symbol $\mathbf{y}_j$, $j \in [0, N-1]$ resulting in $h - s + 1$ interpolation points per received symbol. Instead of using only $h - s + 1$ interpolation points per received symbol $\mathbf{y}_j$, we "overlap" to the neighboring symbol to get h interpolation points per symbol. Since

$\alpha^n \neq \alpha^0$ and $f(\alpha^n) \neq f(\alpha^0)$, we cannot "exceed" the last received symbol $\mathbf{y}_{N-1}$ and wrap around to the first code symbol $\mathbf{y}_0$. Thus we can use only $h - s + 1$ interpolation points for the last symbol. In total we get $Nh - (s-1)$ interpolation points. In the interpolation step we must solve the following problem.

Problem 1 Given an integer $s \in [1, h]$ and a degree constraint D, find a nonzero $(s+1)$-variate linearized polynomial of the form

$$Q(x, y_1, \ldots, y_s) = Q_0(x) + Q_1(y_1) + \cdots + Q_s(y_s) \tag{14}$$

which satisfies the following conditions:

- $Q(\alpha^{jh+i}, y_{jh+i}, y_{jh+i+1}, \ldots, y_{jh+i+s-1}) = 0, \forall i \in [0, h-1], j \in [0, N-2]$,
- $Q(\alpha^{n-h+i}, y_{n-h+i}, y_{n-h+i+1}, \ldots, y_{n-h+i+s-1}) = 0, \forall i \in [0, h-s]$,
- $\deg_q(Q_0(x)) < D$,
- $\deg_q(Q_\ell(y_\ell)) < D - (k-1), \forall \ell \in [1, s]$.

The following example illustrates the choice of the interpolation points in Problem 1.

Example 1 (Interpolation Step) Suppose we transmit a codeword of a folded Gabidulin code with parameters $N = 4$ and $h = 3$ over a rank error channel (6) and we receive a matrix

$$\mathbf{y} = \left(\begin{bmatrix} y_0 \\ y_1 \\ y_2 \end{bmatrix}, \begin{bmatrix} y_3 \\ y_4 \\ y_5 \end{bmatrix}, \begin{bmatrix} y_6 \\ y_7 \\ y_8 \end{bmatrix}, \begin{bmatrix} y_9 \\ y_{10} \\ y_{11} \end{bmatrix} \right).$$

Denote by $\mathcal{I}_{\mathrm{HR}}$ and $\mathcal{I}_{\mathrm{MV}}$ the set of interpolation points for the improved high-rate decoder (Problem 1) and the Mahdavifar–Vardy decoder in [13], respectively. For decoding parameter $s = 2$ we have the following sets of interpolation points:

$$\begin{aligned} \mathcal{I}_{\mathrm{HR}} = \big\{ &(\alpha^0, y_0, y_1), (\alpha^1, y_1, y_2), (\alpha^2, y_2, y_3), \\ &(\alpha^3, y_3, y_4), (\alpha^4, y_4, y_5), (\alpha^5, y_5, y_6), \\ &(\alpha^6, y_6, y_7), (\alpha^7, y_7, y_8), (\alpha^8, y_8, y_9), \\ &(\alpha^9, y_9, y_{10}), (\alpha^{10}, y_{10}, y_{11}) \big\} \end{aligned}$$

$$\begin{aligned} \mathcal{I}_{\mathrm{MV}} = \big\{ &(\alpha^0, y_0, y_1), (\alpha^1, y_1, y_2), \\ &(\alpha^3, y_3, y_4), (\alpha^4, y_4, y_5), \\ &(\alpha^6, y_6, y_7), (\alpha^7, y_7, y_8), \\ &(\alpha^9, y_9, y_{10}), (\alpha^{10}, y_{10}, y_{11}) \big\}. \end{aligned}$$

The improved high-rate decoder uses the interpolation points from the set $\mathcal{I}_{\mathrm{MV}}$ plus three additional interpolation points that wrap around to the neighboring symbols.

A solution to Problem 1 can be found by solving a homogeneous linear system of equations. Denote the component polynomials of (14) by

$$Q_0(x) = \sum_{j=0}^{D-1} q_{0,j} x^{[j]}, \qquad Q_\ell(y_\ell) = \sum_{j=0}^{D-k} q_{\ell,j} y_\ell^{[j]}, \qquad \forall \ell \in [1, s].$$

Let the matrix $\mathbf{T}$ contain all $Nh - (s-1)$ interpolation points from Problem 1 as rows and denote by $\mathbf{t}_\ell$ the ℓth column of $\mathbf{T}$ for $\ell \in [0, s]$. The coefficients of (14) can be found by solving the homogeneous linear system of equations

$$\mathbf{R} \cdot \mathbf{q}_I^T = \mathbf{0} \tag{15}$$

where $\mathbf{R}$ is an $Nh - (s-1) \times D(s+1) - s(k-1)$ matrix

$$\mathbf{R} = \left(\mathbf{M}_D(\mathbf{t}_0^T)^T, \mathbf{M}_{D-k+1}(\mathbf{t}_1^T)^T, \ldots, \mathbf{M}_{D-k+1}(\mathbf{t}_s^T)^T \right) \tag{16}$$

and

$$\mathbf{q}_I = \left(q_{0,0}, \ldots, q_{0,D-1} \mid q_{1,0}, \ldots, q_{1,D-k} \mid \ldots \mid q_{s,0}, \ldots, q_{s,D-k}\right). \tag{17}$$

Lemma 2 *A nonzero polynomial fulfilling the interpolation constraints in Problem 1 exists if*

$$D = \left\lceil \frac{Nh - 2(s-1) + sk}{s+1} \right\rceil. \tag{18}$$

Proof Problem 1 forms a homogeneous system of $Nh-(s-1)$ equations in $D(s+1)-s(k-1)$ unknowns. This system has a nonzero solution if the number of conditions is less than the number of unknowns, i.e., if

$$Nh - (s-1) < D(s+1) - s(k-1) \quad \Longleftrightarrow \quad D \geq \frac{Nh - 2(s-1) + sk}{s+1}. \tag{19}$$

□

We define a univariate polynomial $P(x) \in \mathbb{L}_{q^m}[x]$ as

$$P(x) \stackrel{\text{def}}{=} Q(x, f(x), f(\alpha x), \ldots, f(\alpha^{s-1}x)) = Q_0(x) + \sum_{\ell=1}^{s} Q_\ell(f(\alpha^{\ell-1}x)) \tag{20}$$

where $f(x) \in \mathbb{L}_{q^m}[x]_{<k}$.

Lemma 3 *Let* $\operatorname{rk}\left(\mathbf{e}_0^T, \mathbf{e}_1^T, \ldots, \mathbf{e}_{N-1}^T\right) = t$. *Then the linearized polynomial* $P(x)$ *in* (20) *has at least* $Nh - (s-1) - t(h+s-1)$ *linearly independent roots in* $\mathbb{F}_{q^m}$.

Proof Since $Q(x, y_1, \ldots, y_s)$ is a linearized polynomial we can perform $\mathbb{F}_q$-elementary operations on the set of interpolation points from Problem 1 without affecting its root space. Then by $\mathbb{F}_q$-elementary operations on the set of interpolation points we can have at most $t(h+s-1)$ interpolation points that are corrupted by the rank errors and at least $Nh - (s-1) - t(h+s-1)$ interpolation points of the form

$$\left(\beta_j, f(\beta_j), f(\alpha\beta_j), \ldots, f(\alpha^{s-1}\beta_j)\right)$$

for all $j \in [0, Nh - s - t(h+s-1)]$ that are not corrupted by rank errors. The elements $\beta_j \in \mathbb{F}_{q^m}$ are obtained by $\mathbb{F}_q$-elementary operations on the code locators $\alpha^0, \ldots, \alpha^{n-1}$ and thus linearly independent over $\mathbb{F}_q$. From the interpolation constraints in Problem 1 we have

$$Q\left(\beta_j, f(\beta_j), f(\alpha\beta_j), \ldots, f(\alpha^{s-1}\beta_j)\right) = P(\beta_j) = 0$$

for all $j \in [0, Nh - s - t(h+s-1)]$ which implies that $P(x)$ has at least $Nh - (s-1) - t(h+s-1)$ linearly independent roots in $\mathbb{F}_{q^m}$. □

The result of Lemma 3 is illustrated in Example 2 in the Appendix. The decoding radius for the improved high-rate decoder is expressed as follows.

Theorem 2 *Let* $Q(x, y_1, \ldots, y_s) \neq 0$ *fulfill the interpolation constraints in Problem 1. If the rank of the error matrix* $t = \operatorname{rk}(\mathbf{E})$ *satisfies*

$$t < \frac{s}{s+1}\left(\frac{Nh - k - (s-2)}{h+s-1}\right) \tag{21}$$

then

$$P(x) = Q(x, f(x), f(\alpha x), \ldots, f(\alpha^{s-1}x)) = 0. \tag{22}$$

Proof By Lemma 3 the polynomial $P(x)$ has at least $Nh - (s-1) - t(h+s-1)$ linearly independent roots in $\mathbb{F}_{q^m}$. If we choose

$$D \leq Nh - (s-1) - t(h+s-1) \tag{23}$$

then $P(x)$ has more linearly independent roots than its degree which is only fulfilled if $P(x) = 0$. Combining (19) and (23) we obtain

$$\begin{aligned} Nh - (s-1) + s(k-1) &< (s+1)(Nh - (s-1) - t(h+s-1)) \\ \iff \quad t &< \frac{s}{s+1}\left(\frac{Nh - k - (s-2)}{h+s-1}\right). \end{aligned}$$

□

The normalized decoding radius $\tau_{HR} = t/N$ for the improved high-rate decoding approach is

$$\tau_{HR} < \frac{s}{s+1} \cdot \frac{h}{h+s-1}(1-R) - \frac{s(s-2)}{N(s+1)(h+s-1)}. \tag{24}$$

The "termination loss" $\frac{s(s-2)}{N(s+1)(h+s-1)}$ is caused by the reduced number of interpolation points for the last symbol (no wrap around to the first symbol). The term vanishes with order $1/N$ for large N and h while keeping $s << h$.

Lemma 4 *The optimal decoding parameter s for* $N \to \infty$ *is* $s_{opt} = \sqrt{h-1}$.

Proof For $N \to \infty$ the "termination loss" $\frac{s(s-2)}{N(s+1)(h+s-1)}$ vanishes. In order to maximize the decoding radius choose s such that

$$\begin{aligned} \frac{d}{ds}\tau_{HR}(s,h) &= \frac{d}{ds}\left(\frac{s}{s+1} \cdot \frac{h}{h+s-1}(1-R)\right) \\ &= -\frac{(s^2h - h^2 + h)}{(s^2 + sh + h - 1)^2}(1-R) \stackrel{!}{=} 0. \end{aligned}$$

This is fulfilled for $s = \pm\sqrt{h-1}$ and since $1 \leq s \leq h$ we have $s_{\text{opt}} = \sqrt{h-1}$.

□

For the optimal decoding parameter $s_{opt} = \sqrt{h-1}$ and for $N \to \infty$ we get the maximum normalized decoding radius

$$\tau^*_{HR} \approx \frac{h}{2\sqrt{h-1}+h}(1-R). \tag{25}$$

3.2 Root-finding step

In the root-finding step we must find all polynomials $f(x) \in \mathbb{L}_{q^m}[x]_{<k}$ that are a solution to (22). This corresponds to solving a *linear* system of equations. Define the polynomial $P(x)$ as in (20) and define the polynomials

$$B_i(x) = q_{1,i} + q_{2,i}x + \cdots + q_{s,i}x^{s-1}$$

for $i \in [0, k-1]$. The ith coefficient p_i of $P(x)$ is then equal to

$$p_i = q_{0,i} + f_i B_0(\alpha^{[i]}) + f^{[1]}_{i-1} B_1(\alpha^{[i]}) + \cdots + f^{[i]}_0 B_i(\alpha^{[i]}).$$

The solution space of the interpolation system (15) can have dimension larger than one in general. In this case there exists a *set* of $\mathbb{F}_{q^m}$-linearly independent linearized polynomials with coefficients from $\mathbb{F}_{q^m}$ that are a solution to Problem 1. Similar to [2,19] we use a basis for the solution space of (15) to increase the probability that the root-finding system has full rank. We now lower bound the dimension of the solution space of (15).

Lemma 5 *Let* $\mathrm{rk}(\mathbf{E}) = t$. *Then the dimension* d_I *of the solution space of the interpolation system* (15) *is at least* $s(D-k+1) - t(h+s-1)$.

Proof The first D columns of $\mathbf{R}$ form an $N(h+s-1) \times D$ *Moore* matrix $\mathbf{M}_D(\mathbf{t}_0^T)^T$ of rank D since the elements in $\mathbf{t_0}$ are linearly independent and $D < Nh - (s-1)$. The matrices $\mathbf{M}_{D-k+1}(\mathbf{t}_1^T)^T \ldots \mathbf{M}_{D-k+1}(\mathbf{t}_s^T)^T$ are linear combinations of the columns of $\mathbf{M}_D(\mathbf{t}_0^T)^T$ and thus do not increase the rank. Thus the rank of $\mathbf{R}$ only depends on D and the rank of the error matrix $\mathbf{E}$. By Lemma 3 an error of rank t affects at most $t(h+s-1)$ interpolation points and thus increases the rank of $\mathbf{R}$ by at most $t(h+s-1)$ since $t(h+s-1) < D(s+1) - s(k-1)$. Hence we have $\mathrm{rk}(\mathbf{R}) \leq D + t(h+s-1)$. The dimension of the solution space of the interpolation system (15) is

$$\begin{aligned} d_I \overset{\text{def}}{=} \dim \ker(\mathbf{R}) &\geq D(s+1) - s(k-1) - \mathrm{rk}(\mathbf{R}) \\ &= s(D-k+1) - t(h+s-1). \end{aligned}$$

□

We now set up the root-finding system using d_I polynomials. Define the polynomials

$$B_i^{(\ell)}(x) = q_{1,i}^{(\ell)} + q_{2,i}^{(\ell)} x + q_{3,i}^{(\ell)} x^2 + \cdots + q_{s,i}^{(\ell)} x^{s-1}$$

for $\ell \in [1, d_I]$ and the vectors

$$\mathbf{b}_{i,j} = \left(B_i^{(1)}(\alpha^{[j]}) \; B_i^{(2)}(\alpha^{[j]}) \; \ldots \; B_i^{(d_I)}(\alpha^{[j]}) \right)^T$$

and $\mathbf{q}_{0,i} = \left(q_{0,i}^{(1)} \; q_{0,i}^{(2)} \; \ldots \; q_{0,i}^{(d_I)} \right)^T$ for $i, j \in [0, k-1]$. Defining the root-finding matrix

$$\mathbf{B} = \begin{pmatrix} \mathbf{b}_{0,0} & & & \\ \mathbf{b}_{1,1}^{[-1]} & \mathbf{b}_{0,1}^{[-1]} & & \\ \vdots & \ldots & \ddots & \\ \mathbf{b}_{k-1,k-1}^{[-(k-1)]} & \mathbf{b}_{k-2,k-1}^{[-(k-1)]} & \cdots & \mathbf{b}_{0,k-1}^{[-(k-1)]} \end{pmatrix} \tag{26}$$

and $\mathbf{q} = \left(\mathbf{q}_{0,0} \; \mathbf{q}_{0,1}^{[-1]} \ldots \; \mathbf{q}_{0,k-1}^{[-(k-1)]} \right)^T$, the coefficients of $f(x)$ can be found by solving the truncated system

$$\mathbf{B} \cdot \mathbf{f} = -\mathbf{q} \tag{27}$$

for $\mathbf{f} = \left(f_0 \; f_1^{[-1]} \; \ldots \; f_{k-1}^{[-(k-1)]} \right)^T$. The root-finding system (27) has always a solution if (21) holds since the transmitted message polynomial $f(x)$ is a solution to (22) if t satisfies (21).

Proposition 1 *Solving* (27) *requires at most* $\mathcal{O}(k^2)$ *operations in* $\mathbb{F}_{q^m}$.

Proof The $kd_I \times k$ matrix $\mathbf{B}$ has an upper block triangular structure. To solve (27) we only need one equation per $\mathbf{b}_{i,j}$ for $i, j \in [0, k-1]$ such that $B^{(\ell)}(\alpha^{[j]}) \neq 0$. Thus the system can be solved via back substitution requiring at most $\mathcal{O}(k^2)$ operations in $\mathbb{F}_{q^m}$. □

4 List and unique decoding for high code rates

We show how to use the interpolation-based decoding principle from Sect. 3 as a list decoder or as a probabilistic unique decoder which returns a unique solution with (very) high probability.

4.1 List decoding for high code rates

The solution space of the root-finding system (27) is an affine subspace over $\mathbb{F}_q$. In case the root-finding system (27) is underdetermined, i.e., $\mathrm{rk}(\mathbf{B}) < k$, we obtain a list of possible message polynomials $f(x)$ which satisfy (22).

Lemma 6 *The dimension of the $\mathbb{F}_q$-affine solution space of the root-finding system (27) is at most $m(s-1)$.*

Proof The root-finding matrix $\mathbf{B}$ has full rank if and only if all diagonal elements $\mathbf{b}_{0,0}, \ldots, \mathbf{b}_{0,k-1}$ are nonzero vectors. The entries of each $\mathbf{b}_{0,i}$ are the evaluations of d_I polynomials of degree at most $s-1$ at $\alpha^{[i]}, i \in [0, k-1]$. Since the conjugates $\alpha, \alpha^{[1]}, \ldots, \alpha^{[k-1]}$ are all distinct and $\deg(B_0^{(\ell)}(x)) < s$ for all $\ell \in [1, d_I]$, we can have $\mathbf{b}_{0,i} = \mathbf{0}, i \in [0, k-1]$ at most $(s-1)$ times. For each $\mathbf{b}_{0,i} = \mathbf{0}, i \in [0, k-1]$ the coefficient f_i can be any element in $\mathbb{F}_{q^m}$. Thus we have at most $q^{m(s-1)}$ solutions and the dimension of the $\mathbb{F}_q$-affine solution space is at most $m(s-1)$. □

In the worst case the decoder outputs an exponential number of candidate message polynomials. Using more interpolation polynomials to solve the root-finding system does not reduce the worst case size of the list but helps to reduce the average list size.

We will now derive the average list size for folded Gabidulin codes using similar ideas as in [19] and [14].

Lemma 7 *Let the t fulfill (21). The average list size $\bar{L}_f(t)$ of an h-folded Gabidulin code C, i.e., the average number of codewords in any ball of radius t that contains a codeword, is then upper bounded by*

$$\bar{L}_f(t) < 1 + 4q^{-m(h(N-t)-k)+t(N-t)}. \tag{28}$$

Proof Let $\mathbf{Y} \in \mathbb{F}_q^{hm \times N}$ be a matrix chosen uniformly at random from all matrices in $\mathbb{F}_q^{hm \times N}$. The number of matrices lying within rank distance at most t from $\mathbf{Y}$ in $\mathbb{F}_q^{hm \times N}$ is upper bounded by $|\mathcal{B}^{(t)}(\mathbf{Y})| < 4q^{(mh+N)t-t^2}$ and independent of $\mathbf{Y}$ (see e.g., [18]). If t satisfies (21) we know that the causal (transmitted) codeword is contained in $\mathcal{B}^{(t)}(\mathbf{Y})$. There are $q^{mk}-1$ noncausal codeword matrices out of q^{mhN} possible matrices which can be in $\mathcal{B}^{(t)}(\mathbf{Y})$. Thus there are on average

$$\frac{q^{mk}-1}{q^{mhN}} \cdot |\mathcal{B}^{(t)}(\mathbf{Y})| < \frac{q^{mk}}{q^{mhN}} \cdot 4q^{(mh+N)t-t^2} = 4q^{-m(h(N-t)-k)+t(N-t)}$$

noncausal codewords in $\mathcal{B}^{(t)}(\mathbf{Y})$. Including the causal codeword we get (28). □

4.2 A probabilistic unique decoder for high code rates

The interpolation-based decoding scheme from Sect. 3 can be used as a probabilistic unique decoder. The main idea behind this decoder is to output a unique solution or declare a decoding failure if the list size is larger than one. We will now show that in most cases we obtain a unique solution, i.e., a list of size one.

The root-finding system (22) has a unique solution if $\mathbf{B}$ has rank k which is fulfilled if and only if at least one entry of each $\mathbf{b}_{0,i}$, $i \in [0, k-1]$ is nonzero.

Lemma 8 *Denote by d_I the dimension of the solution space of* (15). *The probability P_e that* $\mathbf{B}$ *is singular is upper bounded by*

$$P_e < k \left(\frac{k}{q^m}\right)^{d_I} = k \left(\frac{k}{q^m}\right)^{s(D-k+1)-t(h-s+1)} \tag{29}$$

under the assumption that the coefficients of the polynomials $B_0^{(1)}(x), \ldots, B_0^{(d_I)}(x)$ are independent and uniformly distributed over $\mathbb{F}_{q^m}$.

Proof Evaluating $B_0^{(\ell)}(x), \forall \ell \in [1, d_I]$ at the conjugates $\alpha, \alpha^{[1]}, \ldots, \alpha^{[k-1]}$ gives ℓ codewords of a (k, s) Reed–Solomon code $\mathcal{C}_{RS}$. The triangular matrix $\mathbf{B}$ has rank k if the diagonal elements are nonzero, i.e., if we get at least one codeword of weight k. Under the assumption that the coefficients of $B_0^{(\ell)}(x)$, $\ell \in [1, d_I]$ are uniformly distributed over $\mathbb{F}_{q^m}$ we get a uniform distribution over the code book of $\mathcal{C}_{RS}$. Using the approximation from [3, Equation 1] the probability P_s to get a codeword of full weight k is

$$P_\mathrm{s} = \frac{\text{no. of weight } k \text{ codewords}}{\text{total no. of codewords}} \approx \frac{\text{no. of weight } k \text{ vectors in } \mathbb{F}_{q^m}^k}{\text{total no. of vectors in } \mathbb{F}_{q^m}^k} = \left(1 - \frac{1}{q^m}\right)^k.$$

The probability that one $B_i^{(\ell)}(\alpha^{[j]})$ in $\mathbf{b}_{0,i}$ is zero is $1 - P_\mathrm{s}$. The coefficients of the polynomials $B_0^{(\ell)}(x)$, $\ell \in [1, d_I]$ are independent by assumption and thus the entries of each $\mathbf{b}_{0,i}$, $i \in [0, k-1]$ also independent. The probability that $\mathbf{b}_{0,i} = \mathbf{0}$, $i \in [0, k-1]$ is upper bounded by

$$(1 - P_\mathrm{s})^{d_I} = \left(1 - \left(1 - \frac{1}{q^m}\right)^k\right)^{d_I} < \left(\frac{k}{q^m}\right)^{d_I}.$$

The probability that at least one $\mathbf{b}_{0,i} = \mathbf{0}$ for $i = 0, \ldots, k-1$ is thus upper bounded by

$$P_e < \Pr\left[\bigcup_{i=0}^{k-1} \mathbf{b}_{0,i} = \mathbf{0}\right] \leq \sum_{i=0}^{k-1} \left(\frac{k}{q^m}\right)^{d_I} = k \left(\frac{k}{q^m}\right)^{d_I}.$$

□

Equation (29) shows that using more polynomials to set up the root-finding system increases the probability that the root-finding matrix $\mathbf{B}$ has full rank, i.e., to get a unique solution. We now relate the dimension of the solution space d_I to the decoding radius and the failure probability. The result is summarized in Theorem 3.

Theorem 3 *Consider an h-folded Gabidulin code* FGab$[h; n, k]$. *Let the coefficients of the polynomials $B_0^{(1)}(x), \ldots, B_0^{(d_I)}(x)$ be independent and uniformly distributed over $\mathbb{F}_{q^m}$. Let*

$\mu > 0$ be an integer. If the rank of the error matrix $t = \mathrm{rk}(\mathbf{E})$ satisfies

$$t \leq \frac{s}{s+1}\left(\frac{Nh-k-(s-2)}{h+s-1}\right) - \frac{\mu}{(s+1)(h+s-1)} \tag{30}$$

then we can find a unique solution $f(x)$ satisfying (22) with probability at least

$$1 - k\left(\frac{k}{q^m}\right)^{\mu}$$

requiring at most $\mathcal{O}(s^2n^2)$ operations in $\mathbb{F}_{q^m}$.

Proof We restrict the dimension of the solution space of the homogeneous interpolation system (15) to be larger than a threshold μ, i.e., $d_I \geq \mu$, and get

$$\mu + t(h+s-1) + s(k-1) \leq Ds. \tag{31}$$

To ensure that $f(x)$ is a root of $P(x)$ in (22), the degree D must satisfy (23). We combine (23) and (31) and get

$$\begin{aligned}\mu + t(h+s-1) + s(k-1) &\leq s(Nh-(s-1)-t(h+s-1)) \\ \iff \quad t &\leq \frac{s}{s+1}\left(\frac{Nh-k-(s-2)}{h+s-1}\right) - \frac{\mu}{(s+1)(h+s-1)}.\end{aligned}$$

The probability of getting a unique solution follows from Lemma 8. The overall complexity is dominated by the interpolation step, which can be solved for $\mu \leq s$ by the efficient algorithm from [2] requiring at most $\mathcal{O}(s^2nD(h-s+1)) < \mathcal{O}(s^2n^2)$ operations in $\mathbb{F}_{q^m}$. □

Theorem 3 shows that there is a tradeoff between the failure probability and the decoding radius. Note that for $\mu = 1$ the decoding radius is equal to the list decoding radius (21). This is a major difference to decoding interleaved Gabidulin codes since probabilistic unique decoding of interleaved Gabidulin codes using only one interpolation polynomial to solve the root-finding system (i.e., $\mu = 1$) is not possible.

The normalized decoding radius $\tau_u = t/N$ for the probabilistic unique decoder is

$$\tau_u \leq \frac{s}{s+1} \cdot \frac{h}{h+s-1}(1-R) - \frac{s(s-2)+\mu}{N(s+1)(h+s-1)}. \tag{32}$$

The decoding radius can be adjusted at the decoder by the choice of the maximum degree of the interpolation polynomials. Substituting (30) in (23) we obtain

$$D(s+1) \leq Nh + s(k-2) + \mu + 1$$

and choose the degree constraint D for the unique decoder

$$D = \frac{Nh + s(k-2) + \mu + 1}{s+1}.$$

The pseudo-code for the probabilistic unique decoding algorithm is given in Algorithm 1. The function *InterpolateBasis*$(\cdot)$ denotes the efficient interpolation algorithm from [2].

Algorithm 1: UniqueDecodeFG($\mathbf{y}$)

Input : $\mathbf{y} = (\mathbf{y}_0, \mathbf{y}_0, \ldots, \mathbf{y}_{N-1}) \in \mathbb{F}_{q^m}^{h \times N}$
Output: A linearized polynomial $f(x) \in \mathbb{L}_{q^m}[x]_{<k}$ or "decoding failure"

Set up $\mathbf{T} \in \mathbb{F}_{q^m}^{Nh-s+1 \times (s+1)}$ to contain all interpolation points of Problem 1 as rows and denote by $\mathbf{t}_0, \ldots, \mathbf{t}_s$ the columns of $\mathbf{T}$
Interpolation step:
$Q^{(1)}, \ldots, Q^{(d_I)} \leftarrow \text{InterpolateBasis}(\mathbf{t}_0^T, \mathbf{t}_1^T, \ldots, \mathbf{t}_s^T)$
Root-finding step:
$Q^* = \{Q^{(\ell)} : \deg_q(Q_0^{(\ell)}) < D \text{ and } \deg_q(Q_j^{(\ell)}) < D - (k-1),\ \ell \in [1, d_I],\ j \in [1, s]\}$
Set up the root-finding matrix $\mathbf{B}$ as in (26) using all polynomials in Q^*
if $\mathbf{b}_{\mathbf{0},\mathbf{i}} \neq \mathbf{0}, \forall i \in [0, k-1]$ **then**
  Find unique solution of the root-finding system $\mathbf{B} \cdot \mathbf{f} = -\mathbf{q}$ and define $f(x)$ from $\mathbf{f}$
  Output: $f(x)$
else
  Output: "decoding failure"

4.3 Performance analysis

We will compare the normalized decoding radius of the decoder from this section to the schemes in [9,13] and [5]. The intersection point of the normalized decoding radii of the decoder in [13] (Mahdavifar–Vardy) and our improved high-rate decoder is

$$\tau_{\text{MV}} = \tau_{\text{HR}} \quad \Longleftrightarrow \quad R = \frac{((N+1)(s-1)-1)(h-s+1)}{2Nh(s-1)}.$$

The high-rate decoder improves upon [13] for code rates $R \geq \frac{((N+1)(s-1)-1)(h-s+1)}{2Nh(s-1)}$ if the same decoding parameter s is used for both decoding algorithms.

In Fig. 1 we consider a folded Gabidulin code with parameters $N = 10, h = 20$ and $s = 6$. Figure 1 shows that the decoder in [13] (Mahdavifar–Vardy) cannot correct rank errors for code rates larger than $\frac{h-s+1}{h} = \frac{3}{4}$.

The decoder for punctured Gabidulin codes (different code construction) in [9] (Guruswami-Xing) has a larger decoding radius for all rates. Due to the structure of the root-finding system in [9] the decoder outputs a basis for all possible candidate polynomials, which is a large list with high probability. Thus this decoder cannot be used as a probabilistic unique decoder. The size of this list was reduced by pre-coding the coefficients of the message polynomials using hierarchical subspace evasive sets in [8] but is still exponential in the length of the code. Note that the code construction by Mahdavifar and Vardy and in this work is the same, whereas the code construction in [9] is different (i.e., no folded Gabidulin code).

Our improved high-rate decoder can correct rank errors for any code rate and will return a list of size one with high probability which is a major benefit for applications. Figure 1 shows that for the given code parameters the scheme improves upon [13] for $R \geq 0.405$ and that the termination loss is already negligible for a code of length $N = 10$.

In Fig. 2 the decoding radius for the optimal decoding parameters for each decoder is plotted. The presented decoding scheme improves upon [13] for $R > 0.45$ for the given code parameters. The figure shows that using $h - s + 1$ interpolation points per symbol that do not wrap around to neighboring symbols (Mahdavifar-Vardy) gives a better decoding performance for low code rates. The improved high-rate decoder uses $(s-1)$ additional

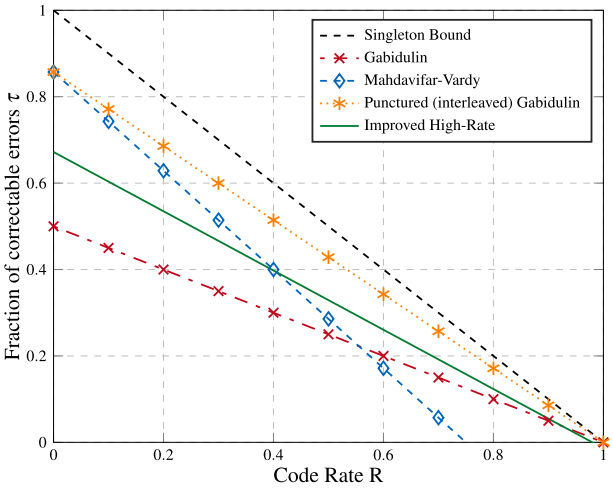

Fig. 1 The normalized decoding radius vs. the code rate R for folded Gabidulin codes with $N = 10$, $h = 20$ and decoding parameter $s = 6$. For comparison we show the decoding radius for punctured Gabidulin codes (Color figure online)

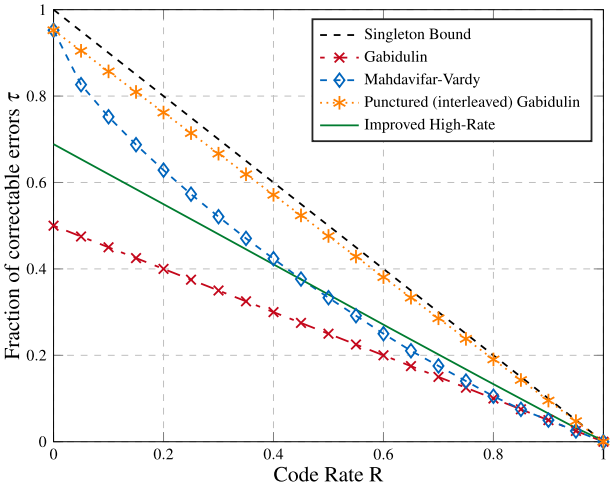

Fig. 2 The normalized decoding radius vs. the code rate R for folded Gabidulin codes with $N = 10$, $h = 20$ and optimal decoding parameter s for each decoder (Color figure online)

interpolation points (i.e., h interpolation points) per symbol (full wrap around) and performs better for high code rates. Using less than the maximum $(s - 1)$ additional interpolation points per symbol that wrap around to the neighboring symbols (partial wrap around) did not improve the decoding radius for any code rate.

4.4 Simulation results

Consider an h-folded Gabidulin code with parameters $m = n = 12, k = 5, h = 3$ and $N = 4$. For parameters $s = 2$ and $\mu = 1$ our decoder can correct $t = 1$ rank errors. We simulated 10^7 transmissions over a rank error channel (6) with $t = 1$ and observed a fraction of $1.10 \cdot 10^{-3}$ decoding failures (upper bound $6.10 \cdot 10^{-3}$). For $\mu = 2$ we simulated $3 \cdot 10^7$

transmissions with $t = 1$ and observed a fraction of $2.06 \cdot 10^{-7}$ decoding failures (upper bound $7.45 \cdot 10^{-6}$). The simulation results show, that the assumptions in the upper bound of that failure probability are reasonable. The average list size using Lemma 7 is upper bounded by $\bar{L}_f(t = 1) < 1 + 1.14 \cdot 10^{-13}$ for the given code parameters.

5 Probabilistic unique decoding of low-rate folded Gabidulin codes

The structure of the root-finding system in the list decoding algorithm by Mahdavifar and Vardy [13] is the same as in our decoding algorithm. We now apply our ideas from Sect. 4 to the list decoding scheme in [13] and present a probabilistic unique decoding scheme for low-rate folded Gabidulin codes. The difference between the approach from Sect. 4 and the Mahdavifar and Vardy decoder is in the choice of the interpolation points. Each $(s+1)$-dimensional interpolation point only contains values strictly chosen from one received symbol $\mathbf{y}_j$, $j \in [0, N-1]$.

Problem 2 *(MV Interpolation Problem)* Given an integer $s \in [1, h]$ and a degree constraint D, find a nonzero $(s+1)$-variate linearized polynomial of the form

$$Q(x, y_1, \ldots, y_s) = Q_0(x) + Q_1(y_1) + \cdots + Q_s(y_s) \tag{33}$$

that satisfies the following conditions:

- $Q(\alpha^{jh+i}, y_{jh+i}, y_{jh+i+1}, \ldots, y_{jh+i+s-1}) = 0, \forall i \in [0, h-s]$, $j \in [0, N-1]$,
- $\deg_q(Q_0(x)) < D$,
- $\deg_q(Q_\ell(y_\ell)) < D - (k-1), \forall \ell \in [1, s]$.

Let the matrix $\mathbf{T}_{\mathrm{MV}}$ contain all $N(h-s+1)$ interpolation points

$$\left(\alpha^{jh+i}, y_{jh+i}, y_{jh+i+1}, \ldots, y_{jh+i+s-1}\right)$$

for all $i \in [0, h-s]$, $j \in [0, N-1]$ from Problem 2 as rows and denote by $\mathbf{t}_{\mathrm{MV},\ell}$ the ℓth column of $\mathbf{T}_{\mathrm{MV}}$ for $\ell \in [0, s]$. The $N(h-s+1) \times (D(s+1) - s(k-1))$ interpolation-matrix $\mathbf{R}_{\mathrm{MV}}$ is defined as

$$\mathbf{R}_{\mathrm{MV}} = \left(\mathbf{M}_D(\mathbf{t}_{\mathrm{MV},0}^T)^T, \mathbf{M}_{D-k+1}(\mathbf{t}_{\mathrm{MV},1}^T)^T, \ldots, \mathbf{M}_{D-k+1}(\mathbf{t}_{\mathrm{MV},s}^T)^T\right) \tag{34}$$

and the coefficient vector $\mathbf{q}_I$ is defined as in (17). The coefficients of the required polynomial can be found by solving the linear system

$$\mathbf{R}_{\mathrm{MV}} \cdot \mathbf{q}_I^T = \mathbf{0}. \tag{35}$$

In order to calculate the dimension of the solution space of (35) we first need to upper bound on the rank of $\mathbf{R}_{\mathrm{MV}}$.

Lemma 9 *Let* $\mathrm{rk}(\mathbf{E}) = t$. *Then the dimension* d_I *of the solution space of the interpolation system* (35) *is at least* $s(D-k+1) - t(h-s+1)$.

Proof By similar arguments as in the proof of Lemma 5 the rank of $\mathbf{R}_{\mathrm{MV}}$ only depends on D and the rank of the error matrix, i.e., $\mathrm{rk}(\mathbf{E}) = t$. An error of rank t corrupts at most $t(h-s+1)$ interpolation points and increases the rank of $\mathbf{R}_{\mathrm{MV}}$ by at most $t(h-s+1)$,

since $t(h-s+1) < D(s+1) - s(k-1)$. Hence we have $\mathrm{rk}(\mathbf{R}_{\mathrm{MV}}) \leq D + t(h-s+1)$. The solution space of (35) has therefore dimension

$$\begin{aligned} d_I \stackrel{\text{def}}{=} \dim \ker(\mathbf{R}_{\mathrm{MV}}) &\geq D(s+1) - s(k-1) - \mathrm{rk}(\mathbf{R}_{\mathrm{MV}}) \\ &= s(D-k+1) - t(h-s+1). \end{aligned}$$

□

Theorem 4 *Consider an h-folded Gabidulin code* $\mathrm{FGab}[h; n, k]$ *and let the coefficients of the polynomials $B_0^{(1)}(x), \ldots, B_0^{(d_I)}(x)$ be independent and uniformly distributed over $\mathbb{F}_{q^m}$. If the rank of the error matrix $t = \mathrm{rk}(\mathbf{E})$ satisfies*

$$t \leq \frac{s(N(h-s+1) - (k-1)) - \mu}{(s+1)(h-s+1)} \tag{36}$$

we can find a unique solution $f(x)$ satisfying (22) with probability at least

$$1 - k\left(\frac{k}{q^m}\right)^{\mu}$$

requiring at most $\mathcal{O}(s^2n^2)$ operations in $\mathbb{F}_{q^m}$.

Proof We restrict the dimension d_I of the solution space of the interpolation system (35) to be larger than a threshold μ, i.e., $\mu \leq d_I$ and get

$$\mu + t(h-s+1) + s(k-1) \leq Ds. \tag{37}$$

To ensure that $f(x)$ is a root of $P(x)$ in (22) the degree D must satisfy (see [13, Corollary 9])

$$D \leq (N-t)(h-s+1). \tag{38}$$

Combining (37) and (38) we get

$$t \leq \frac{s(N(h-s+1) - (k-1)) - \mu}{(s+1)(h-s+1)}. \tag{39}$$

The failure probability follows from Lemma 8. For $\mu \leq s$ the efficient interpolation algorithm from [2] can be used requiring at most $\mathcal{O}(s^2n^2)$ operations in $\mathbb{F}_{q^m}$. □

The normalized decoding radius $\tau_{MV,u} = t/N$ is

$$\tau_{MV,u} \leq \frac{s}{s+1}\left(1 - \frac{h}{h-s+1}R\right) - \frac{\mu - s}{N(s+1)(h-s+1)}.$$

Substituting (39) in (38) we get the degree constraint

$$D \leq \frac{N(h-s+1) - s(k-1) + \mu}{s+1}.$$

This allows to adjust the decoding radius at the decoder by choosing the maximum allowed degree of the interpolation polynomial. For the low-rate probabilistic unique decoder line 1 in Algorithm 1 has to be replaced by

1 Set up $\mathbf{T}_{\mathrm{MV}} \in \mathbb{F}_{q^m}^{N(h-s+1)\times(s+1)}$ to contain all interpolation points of Problem 2 as rows and denote by $\mathbf{t}_{\mathrm{MV},0}, \ldots, \mathbf{t}_{\mathrm{MV},s}$ the columns of $\mathbf{T}_{\mathrm{MV}}$

6 Conclusion

We presented an interpolation-based decoding algorithm for h-folded Gabidulin codes that can correct rank errors beyond half the minimum rank distance for any code rate $0 \leq R \leq 1$. The decoding performance is improved for high-rate codes which is a major benefit for applications. The scheme can be used as a list decoder or as a probabilistic unique decoder which outputs a unique solution with very high probability. We derived an upper bound on the average list size of folded Gabidulin codes and showed that probabilistic unique decoding of folded Gabidulin codes is possible. An efficient decoder with adjustable decoding radius was presented that allows to control the decoding radius vs. failure probability tradeoff. We applied the ideas for the root-finding step to a list decoding algorithm for low-rate folded Gabidulin codes by Mahdavifar and Vardy [13]. This improves the performance when used as probabilistic unique decoder and gives an upper bound on the failure probability.

Acknowledgements The authors would like to thank Gerhard Kramer, Joschi Brauchle and Johan S. R. Nielsen for fruitful discussions and helpful comments. H. Bartz was supported by the German Ministry of Education and Research in the framework of an Alexander von Humboldt-Professorship.

Appendix

Example 2 (Root Space of Interpolation Polynomial) Suppose we transmit a codeword $\mathbf{c}$ of a folded Gabidulin code with parameters $N = 5$ and $h = 3$ and we receive

$$\mathbf{y} = \mathbf{c} + \mathbf{e} = \left(\begin{bmatrix} y_0 \\ y_1 \\ y_2 \end{bmatrix}, \begin{bmatrix} y_3 \\ y_4 \\ y_5 \end{bmatrix}, \begin{bmatrix} y_6 \\ y_7 \\ y_8 \end{bmatrix}, \begin{bmatrix} y_9 \\ y_{10} \\ y_{11} \end{bmatrix}, \begin{bmatrix} y_{12} \\ y_{13} \\ y_{14} \end{bmatrix} \right)$$

where

$$\mathbf{e} = \left(\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} e_1 \\ e_2 \\ e_3 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} e_1 \\ e_2 \\ e_3 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \right)$$

with $t = \mathrm{rk}(\mathbf{e}) = 1$. For decoding parameter $s = 2$ the set of interpolation points from Problem 1 is

$$\begin{aligned} \mathcal{I}_{\mathrm{HR}} = \Big\{ & \big(\alpha^0, f(\alpha^0), f(\alpha^1)\big), && \big(\alpha^1, f(\alpha^1), f(\alpha^2)\big), && \big(\alpha^2, f(\alpha^2), f(\alpha^3) + e_1\big), \\ & \big(\alpha^3, f(\alpha^3) + e_1, f(\alpha^4) + e_2\big), && \big(\alpha^4, f(\alpha^4) + e_2, f(\alpha^5) + e_3\big), && \big(\alpha^5, f(\alpha^5) + e_3, f(\alpha^6)\big), \\ & \big(\alpha^6, f(\alpha^6), f(\alpha^7)\big), && \big(\alpha^7, f(\alpha^7), f(\alpha^8)\big), && \big(\alpha^8, f(\alpha^8), f(\alpha^9) + e_1\big), \\ & \big(\alpha^9, f(\alpha^9) + e_1, f(\alpha^{10}) + e_2\big), && \big(\alpha^{10}, f(\alpha^{10}) + e_2, f(\alpha^{11}) + e_3\big), && \big(\alpha^{11}, f(\alpha^{11}) + e_3, f(\alpha^{12})\big), \\ & \big(\alpha^{12}, f(\alpha^{12}), f(\alpha^{13})\big), && \big(\alpha^{13}, f(\alpha^{13}), f(\alpha^{14})\big) \Big\}. \end{aligned}$$

By performing $\mathbb{F}_q$-elementary operations on $\mathcal{I}_{\mathrm{HR}}$ we eliminate the errors from the interpolation points for the code locators $\alpha^8, \alpha^9, \ldots, \alpha^{11}$ and get the noncorrupted interpolation points

$$\left(\alpha^8-\alpha^2,\, f(\alpha^8-\alpha^2),\, f(\alpha(\alpha^8-\alpha^2))\right), \qquad \left(\alpha^9-\alpha^3,\, f(\alpha^9-\alpha^3),\, f(\alpha(\alpha^9-\alpha^3))\right),$$
$$\left(\alpha^{10}-\alpha^4,\, f(\alpha^{10}-\alpha^4),\, f(\alpha(\alpha^{10}-\alpha^4))\right), \qquad \left(\alpha^{11}-\alpha^5,\, f(\alpha^{11}-\alpha^5),\, f(\alpha(\alpha^{11}-\alpha^5))\right).$$

In total we have $t(h+s-1)=4$ interpolation points that are corrupted by errors and $Nh-(s-1)-t(h+s-1)=10$ noncorrupted interpolation points. The new code locators for the noncorrupted interpolations points are linearly independent over $\mathbb{F}_q$ and thus $P(x)$ must have at least 10 linearly independent roots in $\mathbb{F}_{q^m}$.

References

1. Bartz H.: List and probabilistic unique decoding of high-rate folded Gabidulin codes. In: International Workshop on Coding and Cryptography (WCC) (2015).
2. Bartz H., Wachter-Zeh A.: Efficient interpolation-based decoding of interleaved subspace and Gabidulin codes. In: Proceedings of 52nd Annual Allerton Conference on Communication, Control, and Computing (2014).
3. Cheung K.M.: The weight distribution and randomness of linear codes. TDA Progress Report (42–97), pp. 208–215 (1989).
4. Delsarte P.: Bilinear forms over a finite field with applications to coding Theory. J. Comb. Theory **25**(3), 226–241 (1978).
5. Gabidulin E.M.: Theory of codes with maximum rank distance. Probl. Inf. Transm. **21**(1), 3–16 (1985).
6. Gadouleau M., Yan Z.: Packing and covering properties of rank metric codes. IEEE Trans. Inf. Theory **54**(9), 3873–3883 (2008).
7. Guruswami V., Rudra A.: Explicit codes achieving list decoding capacity: error-correction with optimal redundancy. IEEE Trans. Inf. Theory **54**(1), 135–150 (2008).
8. Guruswami V., Wang C.: Explicit rank-metric codes list-decodable with optimal redundancy. Electron. Colloq. Comput. Complex. (ECCC) **20**, (2013).
9. Guruswami V., Xing C.: List decoding Reed–Solomon, algebraic–geometric, and Gabidulin subcodes up to the singleton bound. Electron. Colloq. Comput. Complex. **19**(146), (2012).
10. Guruswami V., Narayanan S., Wang C.: List decoding subspace codes from insertions and deletions. In: Proceedings of 3rd Innovations in Theoretical Computer Science Conference, ITCS '12, New York, pp. 183–189 (2012). doi:10.1145/2090236.2090252.
11. Lidl R., Niederreiter H.: Finite Fields. Encyclopedia of Mathematics and Its Applications. Cambridge University Press, Cambridge (1996).
12. Loidreau P., Overbeck R.: Decoding rank errors beyond the error correcting capability. In: International Workshop on Algebraic and Combinatorial Coding Theory (ACCT), pp. 186–190 (2006).
13. Mahdavifar H., Vardy A.: List-decoding of subspace codes and rank-metric codes up to Singleton bound. In: IEEE International Symposium on Information Theory (ISIT), pp. 1488–1492 (2012). doi:10.1109/ISIT.2012.6283511.
14. McEliece R.J.: On the average list size for the Guruswami–Sudan decoder. In: International Symposium on Communication Theory and Applications (ISCTA) (2003).
15. Ore Ø.: On a special class of polynomials. Trans. Am. Math. Soc. **35**, 559–584 (1933).
16. Sidorenko V.R., Jiang L., Bossert M.: Skew-feedback shift-register synthesis and decoding interleaved Gabidulin codes. IEEE Trans. Inf. Theory **57**(2), 621–632 (2011).
17. Vadhan S.P.: Pseudorandomness. Found. Trends Theor. Comput. Sci. **7**(13), 1–336 (2011).
18. Wachter-Zeh A.: Bounds on list decoding of rank-metric codes. IEEE Trans. Inf. Theory **59**(11), 7268–7277 (2013).
19. Wachter-Zeh, A., Zeh, A.: List and unique error-erasure decoding of interleaved Gabidulin codes with interpolation techniques. Des. Codes Cryptogr. **73**(2), 547–570 (2014). doi:10.1007/s10623-014-9953-5.