List and Probabilistic Unique Decoding of High-Rate Folded Gabidulin Codes

Hannes Bartz

List and Probabilistic Unique Decoding of High-Rate Folded Gabidulin Codes

Hannes Bartz*

Institute for Communications Engineering
Technische Universität München, Munich, Germany
hannes.bartz@tum.de

Abstract. An efficient interpolation-based decoding algorithm for folded Gabidulin codes is presented that can correct rank errors beyond half the minimum rank distance for any code rate $R \in [0, 1]$. 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 s is a decoding parameter and n is the length of the unfolded code. An upper bound on the average list size and on the decoding failure probability of the decoder is given.

1 Introduction

Decoding schemes for folded Gabidulin codes were independently introduced in [1] and [2]. Both constructions allow to correct rank errors up to the Singleton bound in rank-metric for very small code rates. In [3] it was shown that punctured Gabidulin codes can be decoded up to the Singleton bound for any code rate. An explicit construction and a list decoding algorithm for punctured Gabidulin codes was presented in [4]. This algorithm achieves the best decoding radius for any code rate with a list size exponential in the code length. The output of this decoder is a basis for the affine subspace containing all candidate messages, i.e. a large list with high probability.

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 still exponential, we show that the decoder returns a list of size one with high probability. The scheme can be used 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. In contrast to interleaved Gabidulin codes, probabilistic unique decoding of folded Gabidulin codes up to the full list decoding radius is possible.

* H. Bartz was supported by the German Ministry of Education and Research in the framework of an Alexander von Humboldt-Professorship.

2 Preliminaries

Let q be a power of a prime, and 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 uppercase and lowercase letters such as $\mathbf{A}$ and $\mathbf{a}$ and their elements are indexed beginning from zero. We denote the rank and the row space of a matrix $\mathbf{A} \in \mathbb{F}_q^{m \times n}$ over $\mathbb{F}_q$ by $\mathrm{rk}(\mathbf{A})$ and $\langle \mathbf{A} \rangle$. The kernel of $\mathbf{A}$ is denoted by $\ker(\mathbf{A})$.

For any element $a \in \mathbb{F}_{q^m}$ and any integer i let $a^{[i]} := a^{q^i}$ be the Frobenius power of a. A nonzero polynomial of the form $p(x) = \sum_{i=0}^{d} p_i x^{[i]}$ with $p_i \in \mathbb{F}_{q^m}$, $p_d \neq 0$, is called a *linearized polynomial* of q-degree $\deg_q(p(x)) = d$, see [5, 6]. 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 $p(ax_1 + bx_2) = ap(x_1) + bp(x_2)$. The noncommutative composition $p^{(1)}(x) \otimes p^{(2)}(x) = p^{(1)}(p^{(2)}(x))$ 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 "$\otimes$". 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

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

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 [6].

There is a bijective mapping between any 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 $\mathbb{F}_q$. A rank-metric code $\mathcal{C}$ of length n is a subset of all $m \times n$ matrices over $\mathbb{F}_q$. The minimum rank distance d of $\mathcal{C}$ is defined as

$$d = \min_{\mathbf{x}, \mathbf{y} \in \mathcal{C}} d_r(\mathbf{x}, \mathbf{y}) \stackrel{\text{def}}{=} \min_{\mathbf{x}, \mathbf{y} \in \mathcal{C}} \mathrm{rk}(\mathbf{X} - \mathbf{Y}) \tag{2}$$

where $\mathbf{X}, \mathbf{Y}$ are the matrix representations of $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ over $\mathbb{F}_q$. Denote by $\mathcal{B}^{(\tau)}(\mathbf{Y})$ a ball of radius τ in rank-metric around a matrix $\mathbf{Y}$ containing all matrices in rank distance at most τ from $\mathbf{Y}$.

The Singleton-like bound on the minimum rank distance states that $d \leq n - k + 1$ if $m \geq n$, see [7, 8]. Codes which fulfill this bound with equality are called *maximum rank distance* (MRD) codes. A special class of MRD codes are *Gabidulin codes* [7, 8], which are the analogs of Reed–Solomon codes in rank-metric. As channel model we use the rank error channel

$$\mathbf{Y} = \mathbf{C} + \mathbf{E} \tag{3}$$

where the error matrix $\mathbf{E}$ with $\mathrm{rk}(\mathbf{E}) = t$ is uniformly distributed over all $m \times n$ matrices of rank t over $\mathbb{F}_q$.

Folded Gabidulin codes were proposed independently in [1] and [2]. In [2] 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 [1].

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 $\mathbb{F}_q$. Let h be a positive integer which divides n and denote by $N = n/h$. An h-folded Gabidulin code* $\mathrm{FGab}[h; n, k]$ *of length N, dimension k is defined as*

$$\left\{ \begin{bmatrix} f(\alpha^0) \\ f(\alpha^1) \\ \vdots \\ f(\alpha^{h-1}) \end{bmatrix}, \begin{bmatrix} f(\alpha^h) \\ f(\alpha^{h+1}) \\ \vdots \\ f(\alpha^{2h-1}) \end{bmatrix}, \ldots, \begin{bmatrix} f(\alpha^{n-h}) \\ f(\alpha^{n-h+1}) \\ \vdots \\ f(\alpha^{n-1}) \end{bmatrix} \right\} \tag{4}$$

where $f(x) \in \mathbb{L}_{q^m}[x]$ is a linearized polynomial with $\deg_q < k$.

A codeword of an h-folded Gabidulin code is a matrix $\mathbf{C} \in \mathbb{F}_{q^m}^{h \times N}$ or $\mathbf{C}_q \in \mathbb{F}_q^{hm \times N}$. The j-th column of $\mathbf{C}$ is $\mathbf{c}_j = \big(f(\alpha^{jh}) \ldots f(\alpha^{(j+1)h-1})\big)^T$ for $j \in [0, N-1]$.

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

The proof is omitted due to space restrictions.

3 Improved Interpolation-Based Decoding of High-Rate Folded Gabidulin Codes

The interpolation-based list decoding algorithm in [1] is closely related to the list decoding algorithm for folded Reed-Solomon codes by Guruswami and Rudra [9] and Vadhan [10]. The normalized decoding radius $\tau_{\mathrm{MV}} = t/N$ of this approach is

$$\tau_{\mathrm{MV}} < \frac{s}{s+1} \left(1 - \frac{h}{h-s+1} R \right). \tag{5}$$

Observe that τ_{MV} is positive if $R < \frac{h-s+1}{h}$. Thus the decoder in [1] cannot correct any errors for code rates larger than $\frac{h-s+1}{h}$. But many applications require high-rate codes. We present an improved list decoding scheme that can correct errors beyond the unique decoding radius for any code rate $R > 0$. The scheme is motivated by Justesen's approach for decoding folded Reed-Solomon codes [9, Sec. III-B] and improves upon [1] for high code rates. The code construction remains the same as in Definition 1 but the set of interpolation points is chosen differently.

3.1 Interpolation Step

Suppose we receive a matrix

$$\mathbf{Y} = \left\{ \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{h-1} \end{bmatrix}, \begin{bmatrix} y_h \\ y_{h+1} \\ \vdots \\ y_{2h-1} \end{bmatrix}, \ldots, \begin{bmatrix} y_{n-h} \\ y_{n-h+1} \\ \vdots \\ y_{n-1} \end{bmatrix} \right\}. \tag{6}$$

Denote by $\mathbf{y}_j = (y_{jh}\ y_{jh+1} \dots y_{(j+1)h-1})^T \in \mathbb{F}_{q^m}^h$ the j-th column of $\mathbf{Y}$ for $j \in [0, N-1]$.

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 and wrap around to the first code symbol. Thus we can use only $h-s+1$ interpolation tuples for the last symbol. In total we get $Nh-(s-1)$ interpolation tuples. In the interpolation step we must solve the following problem.

Problem 1. Find a nonzero $(s+1)$-variate linearized polynomial of the form

$$Q\left(x, y_1, \dots, y_s\right) = Q_0(x) + Q_1(y_1) + \dots + Q_s(y_s), \tag{7}$$

which satisfies the following conditions for $s \leq h$:

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

A solution to Problem 1 can be found by solving a homogeneous linear system of equations. Denote the polynomials of (7) by $Q_0(x) = \sum_{j=0}^{d-1} q_{0,j} x^{[j]}$ and $Q_i(y_i) = \sum_{j=0}^{d-k} q_{i,j} y_i^{[j]}$. Let the matrix $\mathbf{T}$ contain all $Nh-(s-1)$ interpolation tuples as rows and denote by $\mathbf{t}_\ell$ the ℓ-th column of $\mathbf{T}$ for $\ell \in [0, s]$. The coefficients of (7) can be found by solving a linear system of equations

$$\mathbf{R} \cdot \mathbf{q}_I^T = \mathbf{0} \tag{8}$$

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

$$\mathbf{R} = \left(\mathbf{M}_d(\mathbf{t}_0^T)^T, \mathbf{M}_{d-k+1}(\mathbf{t}_1^T)^T, \dots, \mathbf{M}_{d-k+1}(\mathbf{t}_s^T)^T\right) \tag{9}$$

and $\mathbf{q}_I = (q_{0,0}, \dots, q_{0,d-1} |\ \dots\ | q_{s,0}, \dots, q_{s,d-k})$.

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

$$d = \left\lceil \frac{Nh - 2(s-1) + sk}{s+1} \right\rceil. \tag{10}$$

Proof. Problem 1 forms a homogeneous system of $Nh-(s-1)$ linearly independent 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

$$Nh-(s-1) < d(s+1)-s(k-1) \quad \Longleftrightarrow \quad d \geq \frac{Nh-2(s-1)+sk}{s+1}. \tag{11}$$

□

The maximum decoding radius for this decoder is expressed as follows.

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

$$t < \frac{s}{s+1}\left(\frac{Nh}{h+s-1} - \frac{k-1}{h+s-1} - \frac{s-1}{h+s-1}\right) \tag{12}$$

then

$$P(x) \stackrel{\text{def}}{=} Q(x, f(x), f(\alpha x), \ldots, f(\alpha^{s-1}x)) = 0. \tag{13}$$

Proof. Since each error of rank one affects $h+s-1$ interpolation points, we have $Nh-(s-1)-t(h+s-1)$ noncorrupted and linearly independent interpolation points. If we choose

$$d \leq Nh - (s-1) - t(h+s-1) \tag{14}$$

then $P(x)$ has more zeros than its degree which is only fulfilled if $P(x) = 0$. Combining (11) and (14) we obtain (12). □

Using the approximation $R \approx \frac{k-1}{Nh}$ the normalized decoding radius τ_{HR} for the improved high-rate decoding approach is

$$\tau_{HR} < \frac{s}{s+1} \cdot \frac{h}{h+s-1}(1-R) - \frac{s(s-1)}{N(s+1)(h+s-1)}. \tag{15}$$

The "termination loss" $\frac{s(s-1)}{N(s+1)(h+s-1)}$ is caused by the reduced number of interpolation points for the last symbol. The term vanishes with order $1/N$ for large N and h while keeping $s << h$.

3.2 Root-Finding Step

In the root-finding step we must find all polynomials $f(x)$ of q-degree less than k which are a solution to (13). This corresponds to solving a *linear* system of equations. Define the polynomial $P(x)$ in (13) as $P(x) = Q_0(x) + \sum_{j=1}^{s} Q_j(f(\alpha^{j-1}x))$ 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 i-th coefficient p_i of $P(x)$ is then equal to

$$p_i = q_{0,i} + f_i B_0(\alpha^{[i]}) + f_{i-1}^{[1]} B_1(\alpha^{[i]}) + \cdots + f_0^{[i]} B_i(\alpha^{[i]}).$$

The solution space of the interpolation system (8) can have dimension larger than one in general. In this case there exists a *set* of linearly independent linearized polynomials which are a solution to Problem 1. Similar to [11,12] we use a basis for the solution space of (8) to increase the probability that the root-finding system has full rank. We now lower bound the dimension of the solution space of (8).

Lemma 3. *Let* $\mathrm{rk}(\mathbf{E}) = \mathrm{rk}\left(\mathbf{E}_1^T, \mathbf{E}_2^T, \ldots, \mathbf{E}_h^T\right)^T = t$. *Then the dimension d_I of the solution space of the interpolation system* (8) *is at least* $s(d-k+1)-t(h+s-1)$.

The proof is omitted due to space restrictions.

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

$$\mathbf{B} = \begin{pmatrix} \mathbf{b}_{0,0} & & & \\ \mathbf{b}_{1,1}^{[-1]} & \mathbf{b}_{0,1}^{[-1]} & & \\ \vdots & \cdots & \ddots & \\ \mathbf{b}_{k-1,k-1}^{[-(k-1)]} & \mathbf{b}_{k-2,k-1}^{[-(k-1)]} & \cdots & \mathbf{b}_{0,k-1}^{[-(k-1)]} \end{pmatrix} \tag{16}$$

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

$$\mathbf{B} \cdot \mathbf{f} = -\mathbf{q} \tag{17}$$

for $\mathbf{f} = \left(f_0 \; f_1^{[-1]} \; \ldots \; f_{k-1}^{[-(k-1)]} \right)^T$. The root-finding system (17) has always a solution if (12) holds.

Proposition 1. *Solving* (17) *requires 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 Section 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

In case the root-finding system (17) is underdetermined, i.e. $\mathrm{rk}(\mathbf{B}) < k$, we obtain a list of possible message polynomials $f(x)$ which satisfy (13).

Lemma 4. *The dimension of the affine solution space of* (17) *is at most* $q^{m(s-1)}$.

The proof is omitted due to space restrictions.

In the worst case the decoder outputs an exponential number of candidate message polynomials. But this does not imply that their evaluation gives codewords in rank distance up to the decoding radius (12). We will now derive the average list size for folded Gabidulin codes using similar ideas as in [11] and [13].

Lemma 5. *Let the decoding radius* τ *fulfill* (12). *The average list size* $\overline{L}_f(\tau)$ *of an* h*-folded Gabidulin code* $\mathcal{C}$ *is then upper bounded by*

$$\overline{L}_f(\tau) < (q^{mk} - 1) \cdot \frac{4q^{(hm+N)\tau - \tau^2}}{q^{mhN}} + 1. \tag{18}$$

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 in rank distance at most τ from $\mathbf{Y}$ in $\mathbb{F}_q^{hm \times N}$ is upper bounded by $|\mathcal{B}^{(\tau)}(\mathbf{Y})| < 4q^{(mh+N)\tau-\tau^2}$ and independent of $\mathbf{Y}$ (see e.g. [14]). If τ satisfies (12) we know that the causal (transmitted) codeword is contained in $\mathcal{B}^{(\tau)}(\mathbf{Y})$. There are $q^{mk}-1$ noncausal codeword matrices out of q^{mhN} possible matrices which can be in $\mathcal{B}^{(\tau)}(\mathbf{Y})$. Thus there are on average

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

noncausal codewords in $\mathcal{B}^{(\tau)}(\mathbf{Y})$. Including the causal codeword we get (18). □

4.2 A Probabilistic Unique Decoder for High Code Rates

The interpolation-based decoding scheme from Section 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 (13) 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 6. *Let the received matrix $\mathbf{Y}$ consist of random elements from $\mathbb{F}_{q^m}$. Denote by d_I the dimension of the solution space of the interpolation system* (8)*. The probability P_e that $\mathbf{B}$ is singular is upper bounded by*

$$P_e < k\left(\frac{k}{q^m}\right)^{d_I} = k\left(\frac{k}{q^m}\right)^{s(d-k+1)-t(h+s-1)}. \tag{19}$$

The proof is omitted due to space restrictions.

Equation (19) shows that using more polynomials to set up the root-finding system increases the probability 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 2.

Theorem 2. *Consider an h-folded Gabidulin code* $\mathrm{FGab}[h; n, k]$*. Let the received matrix $\mathbf{Y}$ consist of random elements from $\mathbb{F}_{q^m}$. Let $\mu > 0$ be an integer. If the rank of the error matrix $t = \mathrm{rk}(\mathbf{E})$ satisfies*

$$t \leq \frac{s}{s+1}\left(\frac{Nh-k-(s-2)}{h+s-1}\right) - \frac{\mu}{(s+1)(h+s-1)} \tag{20}$$

then we can find a unique solution $f(x)$ satisfying (13) *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 interpolation system to be larger than a threshold μ, i.e. $\mu \leq d_I$, and get

$$\mu + t(h + s - 1) + s(k - 1) \leq ds. \tag{21}$$

To ensure that $f(x)$ is a root of $P(x)$ in (13), the degree d must satisfy (14). We combine (14) and (21) and get (20). The probability of getting a unique solution follows from Lemma 6. The overall complexity is dominated by the interpolation step, which can be solved for $\mu \leq s$ by the efficient algorithm from [12] requiring at most $\mathcal{O}(s^2nd(h - s + 1)) < \mathcal{O}(s^2n^2)$ operations in $\mathbb{F}_{q^m}$. □

Theorem 2 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 (12). This is a major difference to decoding interleaved Gabidulin codes since probabilistic unique decoding of interleaved Gabidulin codes up to the full list decoding radius is not possible.

The normalized decoding radius t/N for the probabilistic unique decoder is

$$\tau_u \leq \frac{s}{s+1} \cdot \frac{h}{h+s-1}(1 - R) - \frac{s(s-2) + \mu}{N(s+1)(h+s-1)}. \tag{22}$$

The decoding radius can be adjusted at the decoder by the choice of the maximum degree of the interpolation polynomials. Substituting (20) in (14) we obtain the degree constraint d_u for the unique decoder:

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

4.3 Performance Analysis & Simulation Results

We will compare the normalized decoding radius of the decoder from this section to the schemes in [1], [3] and [8]. Figure 1 shows that the decoder in [1] (Mahdavifar-Vardy) cannot correct rank errors for rates larger than $\frac{h-s+1}{h}$. The construction in [3] (Guruswami-Xing) has a larger decoding radius for all rates. Due to the structure of the root-finding system in [3] the decoder outputs a basis for all possible candidate polynomial, i.e. a large list with high probability. Thus this scheme cannot be used as a probabilistic unique decoder. The size of this list was reduced by using hierarchical subspace evasive sets in [4] but is still exponential in the length of the 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 practical applications. Figure 1 shows that the termination loss is already negligible for a code of length $N = 10$.

Consider an h-folded Gabidulin code with parameters $m = n = 12, k = 5, h = 3$ and $N = 4$. For parameters $s = 2$ and $\mu = 2$ our decoder can correct $t = 1$ rank errors. We simulated $3 \cdot 10^7$ transmissions over a rank error channel (3) with $t = 1$ and observed a fraction of $2.06 \cdot 10^{-7}$ decoding failures (upper bound $7.45 \cdot 10^{-6}$).

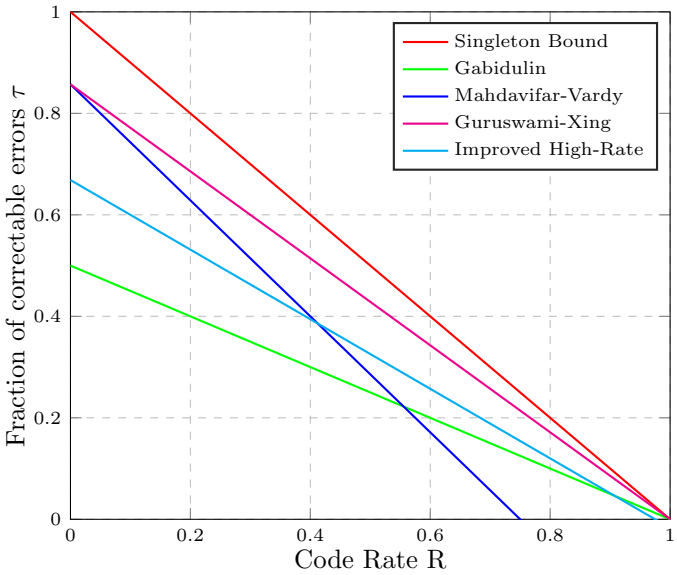

Fig. 1. The normalized decoding radius vs. the code rate for $N=10$, $h=20$ and $s=6$.

5 Conclusion

We presented an interpolation-based decoding algorithm for folded Gabidulin codes that can correct rank errors beyond half the minimum rank distance for any code rate. 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 and showed that probabilistic unique decoding of folded Gabidulin codes up to the list decoding radius is possible. An efficient decoder with adjustable decoding radius was presented that allows to control the decoding radius vs. failure probability tradeoff. Our ideas for the root-finding step can be applied to the decoding algorithm in [1] achieving a decoding radius $t \leq (s(N(h-s+1)-(k-1))-\mu)/((s+1)(h-s+1))$.

Acknowledgment

The author would like to thank Gerhard Kramer, Vladimir Sidorenko and Joschi Brauchle for fruitful discussions and helpful comments.

References

1. H. Mahdavifar and A. Vardy, "List-Decoding of Subspace Codes and Rank-Metric Codes up to Singleton Bound," in *IEEE Trans. Int. Symp. Inf. Theory*, Jul. 2012, pp. 1488–1492.

2. V. Guruswami, S. Narayanan, and C. Wang, "List decoding subspace codes from insertions and deletions," in *Proc. 3rd Innov. in Theoretical Comp. Sci. Conf.*, ser. ITCS '12, New York, NY, USA, 2012, pp. 183–189.
3. V. Guruswami and C. Xing, "List Decoding Reed–Solomon, Algebraic-Geometric, and Gabidulin Subcodes up to the Singleton Bound," *Electr. Colloq. Comp. Complexity*, vol. 19, no. 146, 2012.
4. V. Guruswami and C. Wang, "Explicit Rank-Metric Codes List-Decodable with Optimal Redundancy," *Electr. Coll. on Comp. Complexity (ECCC)*, vol. 20, 2013.
5. Ø. Ore, "On a Special Class of Polynomials," *Trans. Amer. Math. Soc.*, vol. 35, pp. 559–584, 1933.
6. R. Lidl and H. Niederreiter, *Finite Fields*, ser. Encyclopedia of Mathematics and its Applications. Cambridge University Press, Oct. 1996.
7. P. Delsarte, "Bilinear Forms over a Finite Field with Applications to Coding Theory," *J. Combin. Theory*, vol. 25, no. 3, pp. 226–241, 1978.
8. E. M. Gabidulin, "Theory of Codes with Maximum Rank Distance," *Probl. Inf. Transm.*, vol. 21, no. 1, pp. 3–16, 1985.
9. V. Guruswami and A. Rudra, "Explicit Codes Achieving List Decoding Capacity: Error-Correction With Optimal Redundancy," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 135–150, 2008.
10. S. P. Vadhan, "Pseudorandomness," in *Foundations and Trends in Theoretical Computer Science*, 2011.
11. A. Wachter-Zeh and A. Zeh, "List and Unique Error-Erasure Decoding of Interleaved Gabidulin Codes with Interpolation Techniques," *Designs, Codes and Cryptography*, vol. 73, no. 2, pp. 547–570, 2014.
12. H. Bartz and A. Wachter-Zeh, "Efficient Interpolation-Based Decoding of Interleaved Subspace and Gabidulin Codes," in *Proc. 52nd Annual Allerton Conf. Comm., Control, and Comp.*, 2014.
13. R. J. McEliece, "On the Average List Size for the Guruswami–Sudan Decoder," in *Int. Symp. Commun. Theory Appl. (ISCTA)*, 2003.
14. A. Wachter-Zeh, "Bounds on List Decoding of Rank-Metric Codes," *IEEE Trans. Inform. Theory*, vol. 59, no. 11, pp. 7268–7277, Nov. 2013.