EFFICIENT DECODING OF INTERLEAVED SUBSPACE AND GABIDULIN CODES BEYOND THEIR UNIQUE DECODING RADIUS USING GRÖBNER BASES

HANNES BARTZ
Institute of Communications and Navigation
German Aerospace Center (DLR)
D-82234 Oberpfaffenhofen, Germany

ANTONIA WACHTER-ZEH
Institute for Communications Engineering
Technical University of Munich (TUM)
D-80290 Munich, Germany

(Communicated by Sihem Mesnager)

Abstract. An interpolation-based decoding scheme for $L$-interleaved subspace codes is presented. The scheme can be used as a (not necessarily polynomial-time) list decoder as well as a polynomial-time probabilistic unique decoder. Both interpretations allow to decode interleaved subspace codes beyond half the minimum subspace distance. Both schemes can decode $\gamma$ insertions and $\delta$ deletions up to $\gamma + L\delta \leq L(n_t - k)$, where $n_t$ is the dimension of the transmitted subspace and $k$ is the number of data symbols from the field $\mathbb{F}_{q^m}$. Further, a complementary decoding approach is presented which corrects $\gamma$ insertions and $\delta$ deletions up to $L\gamma + \delta \leq L(n_t - k)$. Both schemes use properties of minimal Gröbner bases for the interpolation module that allow predicting the worst-case list size right after the interpolation step. An efficient procedure for constructing the required minimal Gröbner basis using the general Kötter interpolation is presented. A computationally- and memory-efficient root-finding algorithm for the probabilistic unique decoder is proposed. The overall complexity of the decoding algorithm is at most $O(L^2 n_t^2)$ operations in $\mathbb{F}_{q^m}$ where $n_t$ is the dimension of the received subspace and $L$ is the interleaving order. The analysis as well as the efficient algorithms can also be applied for accelerating the decoding of interleaved Gabidulin codes.

1. Introduction

Subspace codes have been proposed as a tool for error correction in noncoherent networks where the network topology and the in-network linear combinations performed by the intermediate nodes are not known by the transmitter and receiver [18,33]. Several code constructions, upper bounds on the size, and properties of such codes were thoroughly investigated in [2,10–12,14,17,18,33–35,41]. Subspace codes with efficient decoding algorithms include the Reed–Solomon (RS)-like code

2010 Mathematics Subject Classification: Primary: 94B35, 94B05.
Key words and phrases: Subspace codes, rank-metric codes, interleaved Gabidulin codes, probabilistic unique decoding, interpolation-based decoding.

A. Wachter-Zeh’s work was supported by the Technical University of Munich—Institute for Advanced Study, funded by the German Excellence Initiative and European Union Seventh Framework Programme under Grant Agreement No. 291763 and the German Research Foundation (Deutsche Forschungsgemeinschaft, DFG) under Grant No. WA3907/1-1.
construction by Kötter and Kschischang [18] (KK) codes and the lifted maximum rank distance (MRD) codes (in particular based on Gabidulin codes, cf. [9, 13, 29]) by Silva, Kötter and Kschischang [33]. For decoding lifted MRD codes, the linear operations performed by the network must be reversed before starting the decoding process. This step is called reduction and allows to apply known error-erasure decoding schemes for MRD codes to lifted MRD codes, but with the additional computational cost of the reduction, see [33].

An interleaved MRD code consists of $L$ matrices, which are codewords of $L$ MRD codes (usually Gabidulin codes). One benefit of using lifted interleaved MRD codes in network coding is a reduced overhead for large interleaving orders. In [22, 30, 39] it was shown that probabilistic unique decoding as well as (not necessarily polynomial-time) list decoding of interleaved Gabidulin codes beyond half the minimum rank distance is possible. The main problem of list decoding subspace and MRD codes is that the list size might be exponential in the code length, see [28, 38]. The approaches of Malavasi and Vardy [23, 24] and Guruswami and Xing [15] provide list decoding schemes for subcodes and modifications of KK and MRD codes. Further, Trautmann, Silberstein and Rosenthal presented an approach for list decoding lifted Gabidulin codes [37]; here the complexity grows exponentially in the dimension of the subspace. Notice that the worst-case list size of many families of MRD codes grows exponentially with the code length, see [28], which therefore rules out polynomial-time list decoding for these code families.

In this paper, we present an interpolation-based decoding scheme for $L$-interleaved KK codes without the need for reduction at the receiver. This approach can be applied as a (not necessarily polynomial-time) list decoder or as a polynomial-time probabilistic unique decoder. The main contribution in this paper is that we show how a Gröbner basis for the interpolation module can increase the performance of the decoder while reducing the computational complexity. An efficient method for constructing minimal Gröbner bases is presented. Using an adapted version of the general linearized polynomial interpolation from [42], the computational complexity of the interpolation step is reduced from $O(Ln_r^2)$ to $O(L^2n_rD) \leq O(L^2n_r^2)$ operations in $\mathbb{F}_{q^m}$, where $n_r$ is the dimension of the received space and $D$ denotes the maximum degree of the constructed polynomial. The interleaving order $L$ is a constant integer which we assume to be small compared to $n_r$. Further, we propose a computationally- and memory-efficient root-finding algorithm for the unique decoder. Given a minimal Gröbner basis for the interpolation module, the algorithm reconstructs the message polynomials in $O(L^2k^2)$ operations in $\mathbb{F}_{q^m}$, where $k$ is the number of data symbols from $\mathbb{F}_{q^m}$. This reduces the computational complexity for the root-finding step compared to $O(L^2k^2)$ for the recursive Gaussian elimination from [39].

Using the proposed algorithms, the total number of operations in $\mathbb{F}_{q^m}$ for the decoder is upper bounded by $O(L^2n_r^2)$. The results are applied to solve the interpolation problem and root-finding system for interleaved Gabidulin codes efficiently [39].

This paper is structured as follows. In Section 2, we give basic definitions and describe notations. Section 3 explains the principle of our interpolation-based decoding algorithm, including calculating the maximum number of tolerated insertions and deletions, and clarifying how we generalize and improve principles from [18]. In Section 4, we outline how our ideas apply to list and unique decoding. Sections 5 and 6 provide efficient interpolation and root-finding algorithms, and Section 7
describes the entire decoding procedure. In Section 8 we compare the proposed decoding algorithm with known decoding schemes for interleaved subspace codes with respect to the error-correction performance and the computational complexity. Finally, Section 9 concludes this paper.

Parts of this work were presented at the 52nd Annual Allerton Conference on Communication, Control, and Computing, Oct. 2014, Monticello, IL, USA [7].

2. Preliminaries

2.1. Finite fields and subspaces. 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 $m$. $\mathbb{F}_q^N$ denotes the vector space of dimension $N$ over $\mathbb{F}_q$ and $\mathcal{P}_q(N)$ is the set of all subspaces of $\mathbb{F}_q^N$. The set of all $\ell$-dimensional subspaces of $\mathbb{F}_q^N$ is called the Grassmannian and is denoted by $\mathcal{G}_q(N, \ell)$.

Matrices and vectors are denoted by bold uppercase and lowercase letters, respectively, such as $\mathbf{A}$ and $\mathbf{a}$. We index vectors and matrices beginning from zero, and $[1, n]$ denotes the set of integers $\{1, 2, \ldots, n\}$. The rank over $\mathbb{F}_q$ and the kernel of a matrix $\mathbf{A} \in \mathbb{F}_q^{m \times n}$ are denoted by $\text{rk}(\mathbf{A})$ and $\ker(\mathbf{A})$, respectively. For any fixed basis of $\mathbb{F}_q^m$ over $\mathbb{F}_q$, there is a bijective mapping between any vector $\mathbf{a} \in \mathbb{F}_q^m$ and a matrix $\mathbf{A} \in \mathbb{F}_q^{m \times n}$. We often switch between these two representations. The row space of a matrix $\mathbf{A} \in \mathbb{F}_q^{m \times n}$ over $\mathbb{F}_q$ is denoted by $\langle \mathbf{A} \rangle_q$. For a column vector $\mathbf{a} \in \mathbb{F}_q^m$ we also use the notation $\langle \mathbf{a} \rangle_q$ to denote the $\mathbb{F}_q$-linear row space $\langle \mathbf{A} \rangle_q$ where $\mathbf{A} \in \mathbb{F}_q^{m \times n}$ is the representation of $\mathbf{a}$ over $\mathbb{F}_q^m$.

The sum $\mathcal{U} + \mathcal{V}$ of two subspaces $\mathcal{U}, \mathcal{V}$ in $\mathcal{P}_q(N)$ is the smallest subspace containing the union of $\mathcal{U}$ and $\mathcal{V}$. The sum $\mathcal{U} + \mathcal{V}$ of two subspaces $\mathcal{U}, \mathcal{V}$ in $\mathcal{P}_q(N)$ is a direct sum (or internal direct sum) $\mathcal{U} \oplus \mathcal{V}$ if $\mathcal{U}$ and $\mathcal{V}$ intersect trivially, i.e. if we have $\mathcal{U} \cap \mathcal{V} = \{0\}$ (see [16]). For a subspace $\mathcal{V} \in \mathcal{G}_q(N, \ell)$ the orthogonal subspace $\mathcal{V}^\perp$ defined as

$$\mathcal{V}^\perp \overset{\text{def}}{=} \{ \mathbf{u} \in \mathbb{F}_q^N : \mathbf{u} \cdot \mathbf{v}^T = 0, \forall \mathbf{v} \in \mathcal{V} \}$$

has dimension $\dim(\mathcal{V}^\perp) = N - \ell$ and we have $\mathcal{V}^\perp \in \mathcal{G}_q(N, N - \ell)$.

The subspace distance between $\mathcal{U}, \mathcal{V}$ in $\mathcal{P}_q(N)$ is

$$d_s(\mathcal{U}, \mathcal{V}) = \dim(\mathcal{U} + \mathcal{V}) - \dim(\mathcal{U} \cap \mathcal{V}) = \dim(\mathcal{U}) + \dim(\mathcal{V}) - 2 \dim(\mathcal{U} \cap \mathcal{V})$$

where the last line follows since $\dim(\mathcal{U} + \mathcal{V}) = \dim(\mathcal{U}) + \dim(\mathcal{V}) - \dim(\mathcal{U} \cap \mathcal{V})$.

A subspace code $\mathcal{C}_s$ is a non-empty subset of $\mathcal{P}_q(N)$, and has minimum subspace distance $d_s$ when all subspaces in the code have distance at least $d_s$ from each other and there is at least one pair of subspaces with distance exactly $d_s$. If every codeword is a subspace of dimension $n_t$ (for “transmitted”), the code is called a constant-dimension code. In the following we only consider constant-dimension codes, i.e. subsets of $\mathcal{G}_q(N, n_t)$.

The code rate of a constant-dimension subspace code $\mathcal{C}_s \subseteq \mathcal{G}_q(N, n_t)$ is defined as

$$R = \frac{\log_q(|\mathcal{C}_s|)}{N n_t}.$$

For a constant-dimension subspace code $\mathcal{C}_s \subseteq \mathcal{G}_q(N, n_t)$ with minimum distance $d_s(\mathcal{C}_s)$ the complementary code\footnote{We use the terminology and notation from [18].} is defined as the set of all orthogonal subspaces
L_\ldots y \text{ in } \deg Q.

The set of all linearized polynomials from \( F_q \) to \( F_q \) with coefficients \( a \in F_q \) is denoted \( \mathcal{L}_a \). We denote the set of all linearized polynomials from \( F_q \) with coefficients \( a \in F_q \) and \( p \in F_q[x] \) with non-commutative composition \( p \circ a(x) = p(a(x)) \) by \( \mathcal{L}_a \circ p \). Given two linearized polynomials \( p_1(x) \) and \( p_2(x) \) of degree \( d_1 \) and \( d_2 \), their non-commutative composition \( p_1(x) \circ p_2(x) = p_1(p_2(x)) \) is a linearized polynomial of degree \( d_1 + d_2 \). The set of all linearized polynomials with coefficients from \( F_q \) forms a non-commutative ring \( \mathbb{L}_{q^n}[x] \) with identity under addition + and composition \( \circ \). We denote the set of all linearized polynomials from \( \mathbb{L}_{q^n}[x] \) to \( \mathbb{L}_{q^n}[x] \) with \( q \)-degree less than \( k \) by \( \mathbb{L}_{q^n}[x]_{<k} \). For a column vector \( a = (a_0 \ a_1 \ldots \ a_{n-1})^T \in F_q^n \) and \( p(x) \in \mathbb{L}_{q^n}[x] \) we define \( p(a) \defeq (p(a_0) \ p(a_1) \ldots \ p(a_{n-1}))^T \).

The set of all multivariate linearized polynomials of the form

\[
Q(x, y_1, \ldots, y_L) = Q_0(x) + Q_1(y_1) + \cdots + Q_L(y_L)
\]

with \( Q_0(x) \in \mathbb{L}_{q^n}[x] \) and \( Q_j(y_j) \in \mathbb{L}_{q^n}[y_j] \) for all \( j \in [1, L] \) is denoted by \( \mathbb{L}_{q^n}[x, y_1, \ldots, y_L] \). For brevity, we also denote the \((L+1)\)-variate linearized polynomial \( Q(x, y_1, \ldots, y_L) \) by \( Q \). Further, for a vector \( w = (w_0, w_1, \ldots, w_L) \), we denote the \( w \)-weighted \( q \)-degree \( \deg_w \) of a multivariate linearized polynomial \( Q \in \mathbb{L}_{q^n}[x, y_1, \ldots, y_L] \) as

\[
\deg_w(Q) \defeq \max \{ w_0 + \deg_Q(Q_0(x)), w_1 + \deg_Q(Q_1(y_1)), \ldots, w_L + \deg_Q(Q_L(y_L)) \}.
\]

The \( q \)-degree is the logarithm to the base \( q \) of the usual degree and thus the weights in \( \deg_w \) are additive instead of multiplicative as in the classical case.
Definition 2.1 (w-Weighted Linearized Monomial Ordering). Given a vector \( \mathbf{w} = (w_0 \ w_1 \ldots \ w_L) \) the w-weighted total order \( \prec_w \) on linearized monomials is defined for all \( j, j' \in [0, L] \) and some \( \ell \geq 0 \) as

\[
y_j^{[\ell]} \prec_w y_{j'}^{[\ell']} \iff \begin{cases} \ell + w_j < \ell + w_{j'} & \text{or} \\ \ell + w_j = \ell' + w_{j'} & \text{and } j < j'. \end{cases}
\]

The w-weighted linearized monomial ordering is also called w-weighted term over position ordering [1] since first the w-weighted degree of the term is considered and the position \( j \) is considered only if two monomials have the same w-weighted degree. To obtain the linearized monomial order \( \prec_w \) for polynomials from \( \mathbb{L}_q[x, y_1, \ldots, y_L] \) we substitute \( y_0 = x \).

For \( \mathbf{w} = (0 \ k - 1 \ldots \ k - 1) \) the total order \( \prec_w \) on linearized monomials is

\[
x^{[\ell+k-1]} \prec_w y_1^{[\ell]} \prec_w y_2^{[\ell]} \prec_w \cdots \prec_w y_L^{[\ell]} \prec_w x^{[\ell+k]}.\]

The set of all polynomials from \( \mathbb{L}_q[x, y_1, \ldots, y_L] \) with weighted degree less than \( D \) is denoted by \( \mathbb{L}_{q}[x, y_1, \ldots, y_L]_{<D} \).

We identify the leading term \( LT(Q) \) of any multivariate polynomial \( Q \) as the maximum monomial under \( \prec_w \) normalized by its coefficient. The index of a univariate polynomial is defined as \( \text{Ind}(l(x) \otimes y_j) = j \) for \( l(x) \in \mathbb{L}_q[x] \). We denote the leading position of a multivariate polynomial \( Q \in \mathbb{L}_q[x, y_1, \ldots, y_L] \) by \( \text{LP}(Q) = \text{Ind}(LT(Q)) \). For a set \( Q \subseteq \mathbb{L}_{q}[x, y_1, \ldots, y_L] \) we denote the set of all leading positions of the elements in \( Q \) by \( \text{LP}(Q) = \{ \text{LP}(Q) : Q \in Q \} \).

The Moore matrix of the vector \( \mathbf{a} = (a_0 \ a_1 \ldots \ a_{n-1}) \in \mathbb{F}_q^n \) is defined as

\[
M_r(\mathbf{a}) = \begin{pmatrix}
a_0 & a_1 & \cdots & a_{n-1} \\
a_0^{[1]} & a_1^{[1]} & \cdots & a_{n-1}^{[1]} \\
\vdots & \vdots & \ddots & \vdots \\
a_0^{[r-1]} & a_1^{[r-1]} & \cdots & a_{n-1}^{[r-1]}
\end{pmatrix}.
\]

The rank of \( M_r(\mathbf{a}) \) is \( \min\{r, n\} \) if the elements \( a_0, \ldots, a_{n-1} \) are linearly independent over \( \mathbb{F}_q \), see [21].

2.3. Lifted Rank-Metric Codes. The minimum rank distance \( d_r \) of a linear code \( \mathcal{C} \subseteq \mathbb{F}_q^n \) is defined as

\[
d_r = \min_{x, y \in \mathcal{C}} d_r(x, y) = \min_{x, y \in \mathcal{C}} \text{rk}(X - Y) = \min_{x \in \mathcal{C}, x \neq 0} \text{rk}(X),
\]

where \( X, Y \) are the matrix representations of \( x, y \in \mathcal{C} \). The Singleton-like bound on the minimum rank distance states that \( d_r \leq n - k + 1 \) when \( m \geq n \), see [9,13,29]. Codes which attain this bound are called MRD codes. A special class of MRD codes are Gabidulin codes [9,13,29], which are the analogs of Reed–Solomon codes in rank metric.

Interleaved Gabidulin codes are a horizontal or vertical concatenation of \( L \) Gabidulin codes, for details see [22,30,39]. If the code rate of all component codes is the same, we call the code a homogeneous \( L \)-interleaved Gabidulin code.

Lifting an (interleaved) MRD code means that we append an identity matrix to each transposed code matrix and consider the row space of these composed matrices as a subspace code. The subspace distance of this constant-dimension code is twice the rank distance of the (interleaved) MRD code [33]. The linear combinations of the received packets at the intermediate nodes in a network coding scenario are
therefore tracked by the leading identity matrix and can be inverted by computing the reduced row echelon form of the received matrix, called reduction.

2.4. Interleaved Kötter-Kschischang Subspace Codes. Motivated by lifted interleaved Gabidulin codes \[20, 31, 39\] and the construction of Kötter and Kschischang \[18\], we define interleaved KK subspace codes as follows.

**Definition 2.2 (L-Interleaved KK Subspace Code).** Let \( a = (a_0\ a_1\ \ldots\ a_{n_t - 1})^T \) with \( n_t \leq m \) be a vector containing \( \mathbb{F}_q \)-linearly independent code locators from \( \mathbb{F}_{q^m} \). For fixed integers \( k^{(1)}, \ldots, k^{(L)} \leq n_t \), an interleaved KK subspace code \( \text{ISub}[L, a; n_t, k^{(1)}, \ldots, k^{(L)}] \) of dimension \( n_t \) and interleaving order \( L \) is defined as

\[
\{ \left( f^{(1)}(a), f^{(2)}(a), \ldots, f^{(L)}(a) \right) \mid f^{(j)}(x) \in \mathbb{L}_{m}[x, k^{(j)}], \forall j \in [1, L] \}.
\]

If \( k^{(j)} = k, \forall j \in [1, L] \) we call the code a homogeneous interleaved KK subspace code and denote it by \( \text{ISub}[L, a; n_t, k] \). The dimension of the ambient vector space is \( N = n_t + Lm \) and the code rate of this construction is

\[
R = \frac{m \sum_{j=1}^{L} k^{(j)}}{n_t(n_t + Lm)}.
\]

For increasing interleaving order \( L \), the rate loss caused by the appended code locators decreases since \( n_t \leq Lm \).

For \( L = 1 \) the codes from Definition 2.2 are equivalent to KK codes \[18\]. The subspace codes over \( \mathbb{F}_{q^L} \) with code locators from \( \mathbb{F}_{q^m} \) in \[15\] are homogeneous \( L \)-interleaved KK subspace codes over \( \mathbb{F}_{q^m} \) (see \[6\]).

**Lemma 2.3 (Minimum Distance).** The minimum subspace distance of an \( L \)-interleaved KK subspace code \( \text{ISub}[L, a; n_t, k^{(1)}, \ldots, k^{(L)}] \) as in Definition 2.2 is

\[
d_{s, \text{min}} = 2 \left( n_t - \max_{j \in [1, L]} \{k^{(j)}\} + 1 \right).
\]

**Proof.** Let \( \mathcal{V} \) and \( \mathcal{V}' \) be two codewords generated by \( f^{(1)}(x), \ldots, f^{(L)}(x) \) and \( g^{(1)}(x), \ldots, g^{(L)}(x) \) with \( q \)-degrees less than \( k^{(1)}, \ldots, k^{(L)} \). Since \( \dim(\mathcal{V}) = \dim(\mathcal{V}') = n_t \) we have

\[
d_s(\mathcal{V}, \mathcal{V}') = 2(n_t - \dim(\mathcal{V} \cap \mathcal{V}')).
\]

Thus the minimum distance is achieved for the maximum dimension of the intersection space \( \mathcal{V} \cap \mathcal{V}' \). The dimension of \( \mathcal{V} \cap \mathcal{V}' \) is minimal when the evaluation polynomials of maximum \( q \)-degree, say \( f^{(j)}(x) \) and \( g^{(j)}(x) \), are distinct and all other evaluation polynomials are identical. Suppose \( \dim(\mathcal{V} \cap \mathcal{V}') = r \), i.e., \( f^{(j)}(x) \) and \( g^{(j)}(x) \) agree on \( r \) linearly independent points. Since two distinct linearized polynomials \( f^{(j)}(x) \) and \( g^{(j)}(x) \) of \( q \)-degree at most \( k^{(j)} - 1 \) can agree on at most \( k^{(j)} - 1 \) linearly independent points (see \[18, Lemma 11\]), it follows that \( r \leq \max\{k^{(j)} - 1\} \). Hence we have

\[
d_{s, \text{min}} = \dim(\mathcal{V}) + \dim(\mathcal{V}') - 2\dim(\mathcal{V} \cap \mathcal{V}')
\geq 2 \left( n_t - \max_{j \in [1, L]} \{k^{(j)}\} + 1 \right).
\]

In order to show that equality holds, let \( f^{(j)}(x) \) and \( g^{(j)}(x) \) be distinct but they agree on exactly \( k^{(j)} - 1 \) points, where \( j \) is chosen such that \( k^{(j)} = \max_i k^{(i)} \).
All other evaluation polynomials are chosen to be equal. Such a choice of \(f^{(i)}(x)\) and \(g^{(i)}(x)\) clearly exists since each polynomial consists of \(k^{(i)}\) coefficients. In this case, we get that the subspace distance between the two codewords generated by \(R(13)\) by solving a linear system of equations that satisfies the following conditions:

\[
\sum_{i=0}^{D-1} q_{0,i} x^{[i]} = \sum_{i=0}^{D-k^{(j)}} q_{j,i} y^{[i]}, \quad \text{for } j \in [1,L].
\]

In the following, we propose an interpolation-based decoding approach for interleaved subspace and Gabidulin codes using Gröbner bases.

### 3. Interpolation-based decoding

In [39] an interpolation-based decoding scheme for interleaved Gabidulin codes that corrects rank errors and row/column erasures was presented. The problem of decoding constant-dimension subspace codes from insertions and deletions can be mapped to a generalized rank-metric decoding problem [32, 33] by computing a canonical form of the basis for the received subspace, called reduction. The interpolation-based scheme proposed in [39] considers lifted interleaved Gabidulin codes and requires the reduction of the received basis (Gaussian elimination) prior to the decoding procedure.

In the following, we propose an interpolation-based decoding approach for interleaved KK subspace codes that generalizes the Kötter-Kschischang approach [18] and is related to interpolation-based decoding of interleaved Gabidulin codes [39]. The decoder takes any basis of the received subspace without the need for the reduction which reduces the complexity at the receiver side. The decoding scheme has an improved decoding performance for insertions compared to [39]. The decoding principle consists of an interpolation step and a root-finding step which are described and analyzed in the following.

#### 3.1. Interpolation step

Suppose we transmit a codeword

\[
Y = \left\{ a \ f^{(1)}(a) \ldots f^{(L)}(a) \right\}_q
\]

over an operator channel (6) with parameters \(\gamma\) and \(\delta\). Let the matrix \(U = (x \ r^{(1)} \ldots r^{(L)}) \in \mathbb{F}_q^{r \times (L+1)}\) contain a basis of the received subspace \(U\) as rows. For the interpolation step, we must solve the following interpolation problem.

**Problem 1** (Interpolation Problem). Given the integers \(n_r, D\) and \(k^{(1)},\ldots,k^{(L)}\), find a nonzero \((L+1)\)-variate linearized polynomial from \(\mathbb{L}_{q^n}[x,y_1,\ldots,y_L]\) of the form

\[
Q(x,y_1,\ldots,y_L) = Q_0(x) + Q_1(y_1) + \cdots + Q_L(y_L),
\]

that satisfies the following conditions:

- \(Q(x_i,r^{(1)}_i,\ldots,r^{(L)}_i) = 0\), \(\forall i \in [0,n_r-1]\),
- \(\deg_q(Q_0(x)) < D\),
- \(\deg_q(Q_j(y_j)) < D - (k^{(j)} - 1)\), \(\forall j \in [1,L]\).

Denote the coefficients of (12) by

\[
Q_0(x) = \sum_{i=0}^{D-1} q_{0,i} x^{[i]} \quad \text{and} \quad Q_j(y_j) = \sum_{i=0}^{D-k^{(j)}} q_{j,i} y_j^{[i]} , \quad \text{for} \ j \in [1,L].
\]

In the following let \(\hat{k} = \sum_{j=1}^{L} k^{(j)}\). We can find the coefficients of \(Q(x,y_1,\ldots,y_L)\) by solving a linear system of equations

\[
R \cdot q^T = 0
\]

Advances in Mathematics of Communications Volume 12, No. 4 (2018), 773–804
Lemma 3.2 (Roots of Interpolation Polynomial). The linearized polynomial $P(x)$ in (17) has at least $n_t - \delta$ linearly independent roots in $\mathbb{F}_q^m$.

Proof. The non-corrupted intersection space $\mathcal{U} \cap \mathcal{V}$ has dimension $n_t - \delta$. Since $f^{(j)}(x), j \in [1, L]$ are linearized polynomials, a basis for $\mathcal{U} \cap \mathcal{V}$ can be represented as

$$\left\{ \left( \xi_i, f^{(1)}(\xi_i), f^{(2)}(\xi_i), \ldots, f^{(L)}(\xi_i) \right) \right\}, i \in [0, n_t - \delta - 1]$$

where $\xi_0, \ldots, \xi_{n_t - \delta - 1}$ are elements from $\mathbb{F}_q^m$ that are linearly independent over $\mathbb{F}_q$. The linearized polynomial $Q(x, y_1, \ldots, y_L)$ vanishes on all elements in the received subspace $\mathcal{U}$. Since $\mathcal{U} \cap \mathcal{V}$ is a subspace of the transmitted space $\mathcal{V}$ we have

$$Q \left( \xi_i, f^{(1)}(\xi_i), f^{(2)}(\xi_i), \ldots, f^{(L)}(\xi_i) \right) = P(\xi_i) = 0$$

for all $i \in [1, n_t - \delta - 1]$ which implies that $P(x)$ has at least $n_t - \delta$ linearly independent roots in $\mathbb{F}_q^m$. 

The following theorem shows that the message polynomials $f^{(1)}(x), \ldots, f^{(L)}(x)$ are roots of $Q(x, y_1, \ldots, y_L)$ under certain constraints.
Theorem 3.3 (Decoding Region). Let $Q(x, y_1, \ldots, y_L) \neq 0$ fulfill the interpolation constraints in Problem 1. Let $\hat{k} = \sum_{j=1}^{L} k^{(j)}$. If
\begin{equation}
\gamma + L\delta < L(n_t + 1) - \hat{k},
\end{equation}
then
\begin{equation}
P(x) = Q(x, f^{(1)}(x), \ldots, f^{(L)}(x)) = 0.
\end{equation}

Proof. By Lemma 3.2, the linearized polynomial $P(x)$ has at least $n_t - \delta$ linearly independent roots in $\mathbb{F}_q$. If we choose
\begin{equation}
D \leq n_t - \delta
\end{equation}
then the dimension of the root space of $P(x)$ in $\mathbb{F}_q$ is larger than its degree. This is possible only if $P(x) = Q(x, f^{(1)}(x), \ldots, f^{(L)}(x)) = 0$. By combining (16) and (20) we have
\begin{align*}
n_t + \hat{k} - L &< D(L + 1) \leq (L + 1)(n_t - \delta) \\
\iff \gamma + L\delta &< L(n_t + 1) - \hat{k}.
\end{align*}

We say that the received subspace is decodable if (18) holds and thus call (18) the decoding region. In other words, the decoding region defines the maximum number of $\gamma$ insertions and $\delta$ deletions where the decoder is able to decode. From (18) we see that interleaving makes the code more resilient against insertions while the performance for decoding deletions remains the same as in [18].

Intuitively, it makes sense that a subspace of dimension $n_t$ with $n_t < N/2$ can tolerate less deletions than insertions. Since its dimension is $n_t$, we can have at most $n_t$ deletions whereas we have at most $N-n_t > N/2$ insertions. For $L$-interleaved KK subspace codes with $n_t \approx m$, we have $N = (L + 1)n_t$ and thus can correct $L$ times more insertions than deletions.

A similar behavior can be observed for the subspace code construction in [15, 24] and the folded subspace codes in [5]. Also, a similar degree of asymmetry can be seen between correctable insertions and deletions in the average list size of interleaved KK subspace codes (see (32)).

For a homogeneous interleaved code $C_s = \text{ISub}[L, a; n_t, k]$ the decoding region is
\begin{equation}
\gamma + L\delta < L(n_t - k + 1)
\end{equation}
\begin{equation}
\iff \gamma + L\delta < L \left( \frac{d_s(C_s)}{2} \right).
\end{equation}

Figure 1 shows the decoding region of a homogeneous 4-interleaved subspace code compared to a Kötter-Kschischang code ($L = 1$) for $d_s = 8$ (i.e. $n_t - k = 7$). The figure illustrates the increased resilience against insertions due to interleaving.

By using the approximation $R \approx \frac{m}{n_t(n_t + Lm)}$ we can express the normalized decoding radius $\tau = \frac{\gamma + L\delta}{n_t}$ as
\begin{equation}
\tau \approx L \left( 1 - \frac{n_t + Lm}{Lm} R \right).
\end{equation}

For $Lm \gg n_t$ the decoding radius approaches $\tau \approx L \left( 1 - R \right)$.

For $L = 1$ the decoding region (18) is the same as in [18, Eq. 11] and improves upon [18] for higher $L$. 

Advances in Mathematics of Communications Volume 12, No. 4 (2018), 773–804
The interpolation-based decoder in [39] uses a basis of the $\mathbb{F}_q^n$-linear solution space of (13) to solve the root-finding step, i.e., to recover the coefficients of the polynomials $f^{(1)}(x), \ldots, f^{(L)}(x)$ from (19).

In our approach we use a so called minimal Gröbner basis for the interpolation module to solve the interpolation system (13) and the root-finding system (19) efficiently.

3.2. Gröbner Bases for the Interpolation Module. Modules over polynomial rings are a generalization of the concept of vectors spaces, where the corresponding vector entries and the scalars are from a polynomial ring. Let $V = \{Q(y_0, y_1, \ldots y_L)\}$ be a free (left) $\mathbb{L}_q^m[x]$-module with a basis $\{y_0, y_1, \ldots, y_L\}$ [42]. Being a free module, any element $Q \in V$ can be represented by $Q = \sum_{j=0}^L Q_j(x) \otimes y_j$, where $Q_j(x) \in \mathbb{L}_q^m[x]$. As in [42], $V$ can be partitioned as $V = \cup_{j} S_j$, where $S_j = \{Q \in V : \text{LP}(Q) = j\}$. Hence, the subset $S_j$ contains all $Q \in V$ with leading position $j$.

Define a set of $n_r$ functionals $F_i : V \rightarrow \mathbb{F}_q^m, i \in [1, n_r]$ such that

$$F_i(Q) = Q \left(x_i, r_i^{(1)}, \ldots, r_i^{(L)}\right), \quad \forall i \in [1, n_r].$$

The kernel of $F_i$ is denoted by $K_i$, and we define $\overline{K}_i = K_1 \cap K_2 \cap \cdots \cap K_i$. Therefore, $\overline{K}_i$ contains all elements $Q \in V$ that are mapped to zero under $F_1, \ldots, F_i$.

Let $T_{i,j} = \overline{K}_i \cap S_j$ contain all elements $Q \in$ from the kernel $\overline{K}_i$ with LP$(Q) = j$. Notice, that all elements in $\overline{K}_{n_r}$ satisfy the first interpolation condition in Problem 1. In particular, all elements from $\overline{K}_{n_r}$ of $w$-weighted degree less than $D$ are a solution for Problem 1.

**Lemma 3.4 (Interpolation Module).** $\overline{K}_{n_r}$ is a left $\mathbb{L}_q^m[x]$-submodule of $V$.

**Proof.** $\overline{K}_{n_r}$ contains all $Q \in V$ that are mapped to zero under $F_i$ for all $i \in [1, n_r]$. For any $l(x) \in \mathbb{L}_q^m[x]$ we have $l(0) = 0$ implying that $l(x) \otimes Q = 0$ for all $Q \in \overline{K}_{n_r}$. Since $F_i$ are linear functionals $F_i(p+q) = F_i(p) + F_i(q) = 0$ holds for any $p, q \in \overline{K}_{n_r}$ and $i \in [1, n_r]$. Thus $\overline{K}_{n_r}$ is closed under addition and the left symbolic product with any element from $\mathbb{L}_q^m[x]$. □

In the following we call $\overline{K}_{n_r}$ the **interpolation module.** Properties of (left) $\mathbb{L}_q^m[x]$-modules and submodules have been studied in [19]. An important observation is,
that \( \overline{K}_{n_r} \) is a free \( \mathbb{L}_q[x] \)-submodule that can be described by a basis as linearized polynomials are a special case of skew polynomials (see [27, Theorem 14]). In this paper we consider a special class of bases, called Gröbner bases, for the free \( \mathbb{L}_q[x] \)-submodule \( \overline{K}_{n_r} \).

**Definition 3.5** (Gröbner Basis [8,19]). Let \( M \) be a left \( \mathbb{L}_q[x] \)-submodule. A subset \( B \subset M \) is called a Gröbner basis for \( M \) under \( \prec_w \) if the leading terms of \( B \) span a left module that contains all leading terms in \( M \).

A Gröbner basis for a \( \mathbb{L}_q[x] \)-submodule \( M \) is not necessarily a minimal generating set for \( M \). The following definition imposes a minimality requirement on the cardinality as well as on the degrees of Gröbner bases for an \( \mathbb{L}_q[x] \)-submodule under a fixed order \( \prec_w \).

**Definition 3.6** (Minimal Gröbner Basis [8]). Given a fixed monomial ordering \( \prec_w \), a Gröbner basis \( \mathcal{G} \) for a left \( \mathbb{L}_q[x] \)-submodule \( M \) is called minimal if for all \( p \in \mathcal{G} \) the leading term \( \text{LT}(p) \) is not contained in the module spanned by \( \text{LT}(\mathcal{G}\setminus\{p\}) \).

**Proposition 1** (Leading Positions of Minimal Gröbner Bases). Let \( \mathcal{G} = \{g_0,g_1,\ldots,g_L\} \) be a minimal Gröbner basis for a left \( \mathbb{L}_q[x] \)-submodule \( M \) w.r.t. a given monomial ordering \( \prec_w \). Then the leading positions of \( g_0,\ldots,g_L \) are distinct.

The proposition follows directly from Definition 3.6 since two polynomials \( g_i, g_j \in \mathcal{G} \) that have the same leading position would contradict that either \( \text{LT}(g_i) \notin \text{LT}(\mathcal{G}\setminus\{g_i\}) \) or \( \text{LT}(g_j) \notin \text{LT}(\mathcal{G}\setminus\{g_j\}) \).

For any \( \mathbb{L}_q[x] \)-submodule there exists a finite minimal Gröbner basis [19, Theorem 12]. We call a minimal Gröbner basis \( \mathcal{G} = \{g_0,g_1,\ldots,g_L\} \) for an \( \mathbb{L}_q[x] \)-submodule ordered if \( \text{LP}(g_j) = j \) holds for all \( j \in [0,L] \). The following lemma relates minimal Gröbner bases for \( \overline{K}_{n_r} \) to the polynomials in the solution space \( \overline{K}_{n_r} \cap \mathbb{L}_q[x,y_1,\ldots,y_L]_{<D} \) of Problem 1.

**Lemma 3.7**. Let \( \mathcal{G} = \{g_0,\ldots,g_L\} \) be an ordered minimal Gröbner basis for the left \( \mathbb{L}_q[x] \)-submodule \( \overline{K}_{n_r} \) under \( \prec_w \) and let \( D \) fulfill (15). Define

\[
\mathcal{G}_{<D} \overset{\text{def}}{=} \{ g \in \mathcal{G} : \deg_w(g) < D \}
\]

Then \( |\mathcal{G}_{<D}| \) satisfies \( 1 \leq |\mathcal{G}_{<D}| \leq L \).

**Proof.** By Lemma 3.1 there exists a polynomial satisfying the constraints in Problem 1 if \( D \) fulfills (15). Since \( \mathcal{G} \) is a minimal Gröbner basis, the minimal (w.r.t. the weighted degree) polynomial among all polynomials satisfying the interpolation constraints is in \( \mathcal{G}_{<D} \) and we have \( |\mathcal{G}_{<D}| \geq 1 \). Since \( \mathcal{G} \) is an ordered minimal Gröbner basis the leading positions of \( g_0, g_1, \ldots, g_L \) are distinct [19, Proposition 7] and hence \( |\mathcal{G}| \leq L+1 \). We now show, that \( g_0 \) is never a solution to the interpolation problem. Let \( g_0 = Q_0(y_0) + Q_1(y_1) + \cdots + Q_L(y_L) \) be nonzero with \( \deg_w(g_0) < D \). Since \( \text{LP}(g_0) = 0 \) (i.e. leading term in \( y_0 \)) we have

\[
\deg_q(Q_0(y_0)) > \max_{j \in [1,L]} \{ \deg_q(Q_j(y_j)) + k(j) - 1 \}.
\]

In order to fulfill \( Q(x,f^{(1)}(x),\ldots,f^{(L)}(x)) = 0 \) with \( \deg_q(f^{(j)}(x)) < k(j) \) for \( j \in [1,L] \),

\[
\deg_q(Q_0(y_0)) \leq \max \{ \deg_q(Q_j(y_j)) + k(j) - 1 \}
\]

must hold, which contradicts (24). Thus we must have \( \deg_w(g_0) \geq D \) and \( g_0 \) is never contained in \( \mathcal{G}_{<D} \). Hence, \( |\mathcal{G}_{<D}| \leq L \). \qed
The proof of Lemma 3.7 shows that a polynomial with leading position 0 (i.e. leading term in \( y_0 \)) is never a solution to the interpolation problem and thus never contained in \( \mathcal{G}_< D \).

**Lemma 3.8.** Let \( \mathcal{G} \) be a minimal Gröbner basis for \( \mathcal{K}_{n_r} \) under \( \prec_w \). Then all solutions \( Q \in \mathbb{L}_{q^m}[x, y_1, \ldots, y_L]_{<D} \) of Problem 1 are of the form

\[
Q = \sum_{i=1}^{[\mathcal{G}_< D]} a_i(x) \otimes Q^{(i)}, \quad Q^{(i)} \in \mathcal{G}_< D
\]

for some \( a_i(x) \in \mathbb{L}_{q^m}[x] \).

**Proof.** Let the set \( J = \text{LP}(\mathcal{G}_< D) \) contain the leading positions of the elements in \( \mathcal{G}_< D \) and let \( J' = \text{LP}(\mathcal{G} \setminus \mathcal{G}_< D) \). Since \( \mathcal{G}_< D \) is a subset of the minimal Gröbner basis \( \mathcal{G} \) the leading positions of the elements in \( \mathcal{G}_< D \) are all distinct implying that the sets \( J \) and \( J' \) are disjoint. We now show that there exists no element in the module generated by \( \mathcal{G} \setminus \mathcal{G}_< D \) that has \( w \)-weighted degree less than \( D \). Suppose there exists a \( q \) in the module generated by \( \mathcal{G} \setminus \mathcal{G}_< D \) with \( \text{deg}_w(q) < D \). If \( \text{LP}(q) \in J \) then we must have that \( q \) is an element in the module generated by \( \mathcal{G}_< D \). If \( \text{LP}(q) \in J' \) then we have that \( q \) is in the module generated by \( \mathcal{G} \). For all \( g \in \mathcal{G} \setminus \mathcal{G}_< D \) we have \( \text{LP}(g) \in J \) and \( \text{deg}_w(g) \geq D \) since otherwise \( g \) would be contained in \( \mathcal{G}_< D \). Thus we have

\[
\text{deg}_w(q) < D \leq \text{deg}_w(g), \quad \forall g \in \mathcal{G} \setminus \mathcal{G}_< D
\]

which implies that \( \text{LT}(q) \) is not contained in the module generated by \( \text{LT}(\mathcal{G}) \). This contradicts the assumption that \( \mathcal{G} \) is a minimal Gröbner basis for \( \mathcal{K}_n \) since by definition we must have that \( \text{LT}(\mathcal{G}) \) and \( \text{LT}(\mathcal{K}_n) \) span the same module. Hence all elements in \( \mathbb{L}_{q^m}[x, y_1, \ldots, y_L]_{<D} \) must be \( \mathbb{L}_{q^m}[x] \)-linear combinations of the elements in \( \mathcal{G}_< D \).

Thus every polynomial in the \( \mathbb{F}_{q^m} \)-linear solution space of (13) can be constructed by an \( \mathbb{L}_{q^m}[x] \)-linear combination of the polynomials in \( \mathcal{G}_< D \) which implies that \( d_I \geq [\mathcal{G}_< D] \).

Clearly, the set \( \mathcal{K}_{n_r} \cap \mathbb{L}_{q^m}[x, y_1, \ldots, y_L]_{<D} \) is not a submodule of \( V \), since an \( \mathbb{L}_{q^m}[x] \)-linear combination of the form \( \sum_{i=1}^{[\mathcal{G}_< D]} a_i(y_0) \otimes Q^{(i)} \) for any \( a_i(x) \in \mathbb{L}_{q^m}[x] \) may result in a polynomial of \( w \)-weighted degree larger than \( D - 1 \).

### 3.3. Root-Finding Step Using Minimal Gröbner Bases

The task of the root-finding step is to find all polynomials \( f^{(j)}(x) \) with \( \text{deg}_q(f^{(j)}(x)) < k^{(j)}, \forall j \in [1, L] \), such that (19) holds. Similar to [39], this is done by solving a linear system of equations in \( \mathbb{F}_{q^m} \) for the coefficients of \( f^{(1)}(x), \ldots, f^{(L)}(x) \).

Instead of using a basis for the \( \mathbb{F}_{q^m} \)-linear solution space of (13) we use a subset of a minimal Gröbner basis of the \( \mathbb{L}_{q^m}[x] \)-submodule \( \mathcal{K}_{n_r} \) to solve the root-finding step. Let \( \mathcal{G} \) be an ordered minimal Gröbner basis for \( \mathcal{K}_{n_r} \) and define the set \( \mathcal{G}_< D \subseteq \mathcal{G} \) as in (23). List decoding of rank-metric codes using Gröbner bases was also considered in [36]; however only for the non-interleaved case \( (L = 1) \).

We now set up the root-finding matrix using \( r = [\mathcal{G}_< D] \) polynomials \( Q^{(i)}(x, y_1, \ldots, y_L) \in \mathcal{G}_< D, \ell \in [1, r] \). Denote the coefficients of the polynomials \( Q^{(i)} \in \mathcal{G}_< D \) by

\[
Q^{(i)}_0(x) = \sum_{i=0}^{D-1} q^{(i)}_0(i) x^i \quad \text{and} \quad Q^{(i)}_{j}(y_j) = \sum_{i=0}^{D-k^{(i)}} q^{(i)}_{j,i} y_j^i.
\]
for all \( \ell \in [1, r] \). Let \( k = \max_{j \in [1, L]} \{ k^{(j)} \} \) and \( \tilde{k} = \min_{j \in [1, L]} \{ k^{(j)} \} \). Define \( Q_{[i]} \) as:

\[
Q_{[i]} = \begin{pmatrix}
q^{(1)}_{1,i} & q^{(1)}_{2,i} & \cdots & q^{(1)}_{L,i} \\
\vdots & \vdots & \ddots & \vdots \\
q^{(r)}_{1,i} & q^{(r)}_{2,i} & \cdots & q^{(r)}_{L,i}
\end{pmatrix},
\]

\[
f^{[i]}_{j} = \begin{pmatrix} f^{(1)}_{j} \cdots f^{(L)}_{j} \end{pmatrix}^T \quad \text{and} \quad q_{0,j}^{[i]} = \begin{pmatrix} q^{(1)}_{0,j} \cdots q^{(r)}_{0,j} \end{pmatrix}^T.
\]

We assume that \( f^{(j)}_{i} = 0 \) for all \( i \geq k^{(j)} \) and \( q_{j,i}^{(\ell)} = 0 \) for \( i > D - k^{(j)} \) for all \( \ell \in [1, r] \). The root-finding matrix can be set up as

\[
Q = \begin{pmatrix}
Q_{0}^{[0]} & Q_{1}^{[-1]} & \cdots & Q_{D-k}^{[-(D-k)]} \\
\vdots & \vdots & \ddots & \vdots \\
Q_{D-k}^{[-(D-k)]} & \cdots & \vdots & \vdots
\end{pmatrix}
\]

and the roots can be found by solving the system of equations

\[
Q \cdot \begin{pmatrix} f_{0}^{[-1]} \cdots f_{k-1}^{[-(k-1)]} \end{pmatrix}^T = -\begin{pmatrix} q_{0,0} \cdots q_{0,D-1} \end{pmatrix}^T.
\]

Solving the root-finding system (27) recursively requires at most \( O(L^3k^2) \) operations in \( \mathbb{F}_q^m \) (see [39]). In Section 6 we present an efficient root-finding algorithm that solves (27) in \( O(L^2k^2) \) operations in \( \mathbb{F}_q^m \).

The following lemma lower bounds the rank of the root-finding matrix (26) by using the properties of the minimal Gröbner basis polynomials.

**Lemma 3.9 (Rank of Root-Finding Matrix).** Let the set \( J = \text{LP}(\mathcal{G}_{<D}) \) contain the leading positions of the polynomials in \( \mathcal{G}_{<D} \). Then the rank of the root-finding matrix \( Q \) in (26) satisfies \( \text{rk}(Q) \geq \sum_{j \in J} k^{(j)} \).

**Proof.** Suppose w.l.o.g. that \( \text{deg}_{\text{mw}}(Q^{(\ell)}) = D-1 \) for all \( \ell \in [1, |\mathcal{G}_{<D}|] \). (In case some \( Q^{(\ell)} \) have weighted degree less than \( D - 1 \) we can increase the degree to \( D - 1 \) by the composition \( x^{[\Lambda]} \otimes Q^{(\ell)} \) with some appropriate \( x^{[\Lambda]} \) without changing \( \text{LP}(Q^{(\ell)}) \) and the number of solutions of \( Q^{(\ell)}(x, f^{(1)}(x), \ldots, f^{(L)}(x)) = 0 \). Let \( Q_{S,j}^{(j)}(D-k) \) be the submatrix of \( Q \) consisting of the \( k^{(j)} \) columns corresponding to the unknown coefficients \( f^{(j)}_{0,1}, f^{(j)}_{1,1}, \ldots, f^{(j)}_{k^{(j)}-1,1} \) and \( k^{(j)} \) rows containing Frobenius powers of the (leading) coefficient \( Q^{(\ell)}_{j,D-k} \) for each \( j \in J \) and some \( \ell \in [1, L] \). Then each \( Q_{S,j}^{(j)} \) is a \( k^{(j)} \times k^{(j)} \) upper triangular matrix with \( Q_{j, D-k}^{(j)} \) on the diagonal. Since each polynomial \( Q^{(j)} \in \mathcal{G}_{<D} \) with \( \text{LP}(Q^{(j)}) = j \) has a nonzero leading coefficient \( Q^{(j)}_{j,D-k} \), the elements \( Q_{j, D-k}^{(j)} \) on the diagonal are nonzero and we have \( \text{rk}(Q_{S,j}^{(j)}) = k^{(j)} \) for all \( j \in J \).

Since \( \mathcal{G}_{<D} \) is a subset of the minimal Gröbner basis \( \mathcal{G} \) the leading positions \( \text{LP}(Q^{(\ell)}) \) are distinct for all \( \ell \in [1, |\mathcal{G}_{<D}|] \). Let \( j_\ell \) for \( \ell \in [1, |\mathcal{G}_{<D}|] \) be the indices of the leading terms of the polynomials in \( \mathcal{G}_{<D} \) and let \( r = |\mathcal{G}_{<D}| \). Then we can set
up an upper block triangular root-finding subsystem of (18) of the form
\[
\begin{pmatrix}
Q_S^{(j_1)} & \cdots & \cdots & Q_S^{(j_r)} \\
\vdots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \vdots \\
Q_S^{(j_r)} & \cdots & \cdots & \cdots
\end{pmatrix}
\begin{pmatrix}
f_0^{(j_1)} \\
f_1^{(j_1)} \\
f_2^{(j_1)} \\
\vdots \\
f_0^{(j_r)} \\
f_1^{(j_r)} \\
f_2^{(j_r)}
\end{pmatrix} = -\tilde{\mathbf{q}}_0^T
\]
for some $\tilde{\mathbf{q}}_0^T$ obtained from $\mathbf{q}_0^T$. We have $\text{rk}(Q_S^{(j)}) = k^{(j)}$ for all $j \in J$ and thus conclude that $\text{rk}(Q) \geq \text{rk}(\tilde{Q}) \geq \sum_{j \in J} k^{(j)}$ where the first inequality follows from the fact that we only considered a submatrix of $Q$. 

Equipped with Lemma 3.9 we can upper bound the dimension of the affine solution space of (27).

**Theorem 3.10 (Maximum List Size).** Let $\mathcal{G} = \{g_0, \ldots, g_L\}$ be a minimal Gröbner basis for the left $L_{q}[x]$-module $\overline{K}_{n_{w}}$ under $\prec_w$. Let $\mathcal{G}_{\prec D} \overset{\text{def}}{=} \{g \in \mathcal{G} : \deg_w(g) < D\} = \{Q^{(1)}, \ldots, Q^{(|\mathcal{G}_{\prec D}|)}\}$ where $D$ satisfies (15). Denote by $\mathcal{J} = \text{LP}(\mathcal{G} \setminus \mathcal{G}_{\prec D})$ the set of leading positions of the polynomials in $\mathcal{G}$ that are not contained in $\mathcal{G}_{\prec D}$. Then the linear system of equations
\[
Q^{(\ell)} (x, f^{(1)}(x), \ldots, f^{(L)}(x)) = 0, \quad \forall \ell \in [1, |\mathcal{G}_{\prec D}|]
\]
has at most $q^{m(\sum_{j \in \mathcal{J}} k^{(j)})}$ solutions.

**Proof.** The dimension of the affine solution space of (27) over $\mathbb{F}_{q^n}$ is $\sum_{j=1}^L k^{(j)} - \text{rk}(Q)$. Let the set $J = \text{LP}(\mathcal{G}_{\prec D})$ contain the leading positions of the polynomials in $\mathcal{G}_{\prec D}$. By Lemma 3.9 we have rank $Q \geq \sum_{j \in J} k^{(j)}$ and thus we can have at most $q^{m(\sum_{j=1}^L k^{(j)} - \sum_{j \in J} k^{(j)})} = q^{m(\sum_{j \in \mathcal{J}} k^{(j)})}$ solutions. 

For the homogeneous case $k^{(j)} = k, \forall j \in [1, L]$ we have at most $q^{m(kL - k(|\mathcal{G}_{\prec D}|))} = q^{mk(L - |\mathcal{G}_{\prec D}|)}$ solutions.

### 4. Application to List and Unique Decoding

#### 4.1. List Decoding Approach.

In general, the root-finding matrix $Q$ (26) does not always have full rank. In this case, we obtain a list of roots of (19), i.e., a list of possible (interleaved) message polynomials. This decoder is not a polynomial-time list decoder but it provides with quadratic complexity the basis of the list.

An important benefit of using a Gröbner basis for the root-finding step is that Theorem 3.10 shows that the actual list size can be upper bounded if $\mathcal{G}_{\prec D}$ is known. Hence, the actual list size can be upper bounded right after interpolating a minimal Gröbner basis for $\overline{K}_{n_{w}}$ without checking the rank of the root-finding matrix (26). This feature is useful if the list decoder is operated such that it declares a decoding failure if the actual list size is too large (i.e., exceeds a defined threshold).

The worst-case list size for the decoder is upper bounded as follows.

---

**Advances in Mathematics of Communications**  Volume 12, No. 4 (2018), 773–804
Lemma 4.1 (Maximum List Size). Let $Q$ be as defined in (26). Then the number of solutions of the root-finding system (27) is at most
\[ q^{m (\sum_{j=1}^{L} k^{(j)} - \min_{j \in [1,L]} k^{(j)})} \]
Proof. From Lemma 3.7 we know, that $|\mathcal{G}| \geq 1$. By Theorem 3.10 the root-finding system (27) has at most $q^{m (\sum_{j=1}^{L} k^{(j)} - \min_{j \in [1,L]} k^{(j)})}$ solutions which is maximized for $J = \arg \min_{j \in [1,L]} \{k^{(j)}\}$. \[ \]

For the homogeneous case $k^{(j)} = k, \forall j \in [1,L]$ this gives $q^{m (Lk-k)} = q^{m(k-1)}$.

Although the root-finding system (27) can have up to $q^{m (\sum_{j=1}^{L} k^{(j)} - \min_{j \in [1,L]} k^{(j)})}$ solutions, not all solutions necessarily give codewords in subspace distance up to the decoding region. Thus the proposed decoding scheme is not necessarily a polynomial time decoder since in the worst case the list size is exponential. However, this decoding scheme computes in polynomial time a basis for the list of all codewords in the decoding region (18).

We now estimate the average number of codewords in the decoding region (18) to show that the probability to obtain a list of exponential size is very small.

Lemma 4.2 (Average List Size). Let $\text{ISub}[L,a;n_t,k]$ be an interleaved $KK$ subspace code over $\mathbb{F}_q$. Let the number of insertions $\gamma$ and deletions $\delta$ fulfill (18). The average list size $\mathcal{L}_I(\gamma, \delta)$, i.e. the average number of codewords in subspace distance at most $\gamma + \delta$ from an $n_t$-dimensional received subspace, is upper bounded by
\[ \mathcal{L}_I(\gamma, \delta) < 1 + 16 \cdot (\min\{\gamma, \delta\} + 1) \cdot q^{L(mk-(n_t-\gamma - \delta)(m-\frac{\gamma}{2}))}. \]
Proof. Let the received subspace $\mathcal{Y}$ be chosen uniformly at random from all subspaces in the Grassmannian $G_q(N,n_t)$, where $N = n_t + Lm$. The number of $n_t$-dimensional subspaces in subspace distance at most $\gamma + \delta$ from the $n_t$-dimensional received space $\mathcal{Y}$ is (see [11, Lemma 7])
\[ V_S(n_t, n_t, \gamma + \delta) = \sum_{j=n_t-\delta}^{\min\{n_t,n_r\}} q^{(n_t-j)(n_r-j)} \left( \begin{array}{c} n_r \\ j \end{array} \right) \left( \begin{array}{c} N - n_t \\ n_t - j \end{array} \right). \]
If $\gamma$ and $\delta$ satisfy (18) we know that the causal (transmitted) codeword is in subspace distance at most $\gamma + \delta$ from $\mathcal{Y}$. There are $q^{mLk-1}$ noncausal codewords (subspaces) out of $\left( \begin{array}{c} N \\ n_t \end{array} \right)$ possible $n_t$-dimensional subspaces. Thus there are on average
\[ \mathcal{T}_I(\gamma, \delta) = \frac{q^{mLk-1} - 1}{\left( \begin{array}{c} N \\ n_t \end{array} \right)} \cdot V_S(n_t, n_t, \gamma + \delta) < \frac{q^{mLk}}{\left( \begin{array}{c} N \\ n_t \end{array} \right)} \cdot V_S(n_t, n_t, \gamma + \delta) \]
\[ < 16 \cdot (\min\{\gamma, \delta\} + 1) \cdot q^{mLk-n_t(N-n_t)+n_t(\gamma-\delta)+\delta(N-\gamma)} \]
\[ < 16 \cdot (\min\{\gamma, \delta\} + 1) \cdot q^{mLk-n_t(N-n_t-\gamma+\delta)+\delta(N-\gamma)} \]
subspaces in subspace distance at most $\gamma + \delta$ from the $n_t$-dimensional received space $\mathcal{Y}$ where (a) follows by using [3, Lemma 3.2]. For $N = n_t + Lm$ we have
\[ \mathcal{T}_I(\gamma, \delta) < 16 \cdot (\min\{\gamma, \delta\} + 1) \cdot q^{mLk-n_t(N+Lm-n_t-\gamma+\delta)+\delta(n_t+Lm-\gamma)} \]
\[ = 16 \cdot (\min\{\gamma, \delta\} + 1) \cdot q^{L(mk-(n_t-\gamma)(m-\frac{\gamma}{2}))}. \]
Including the causal codeword we get $\mathcal{T}_I(\gamma, \delta) = 1 + \mathcal{T}_I(\gamma, \delta)$. \[ \]
Note that if we choose \( n_t \approx m \) in (30), we observe an asymmetry between insertions and deletions of degree \( L \), i.e., deletions affect the average list size of the code \( L \) times more than insertions.

Consider a homogeneous interleaved KK subspace code \( C_s = \text{ISub}[L, a; n_t, k] \). To decode interleaved subspace codes with a probabilistic unique decoder we require the average list size to be close to one. This is fulfilled if the exponent in (30) becomes negative, i.e., if we have

\[
mk - (n_t - \delta) \left( m - \frac{\gamma}{L} \right) < 0
\]

\[
\iff mk < n_t m - n_t \frac{\gamma}{L} - \delta m + \frac{\delta \gamma}{L}
\]

\[
\iff k < n_t - \frac{n_t \gamma}{m} L - \delta + \frac{\delta \gamma}{Lm}.
\]

For \( n_t \approx m \) we get

\[
\frac{\gamma}{L} + \delta < n_t - k + \frac{\delta \gamma}{Lm} \iff \gamma + L \delta < L (n_t - k) + \frac{\delta \gamma}{m}
\]

\[
\iff \gamma + \delta \left( L - \frac{\gamma}{m} \right) < L (n_t - k)
\]

\[
\iff \gamma + \delta \left( L - \frac{\gamma}{m} \right) < L \left( \frac{d_s(C_s) - 2}{2} \right)
\]

(32)

Note, that the decoding region of the list decoder (18) shows a similar order of asymmetry between insertions and deletions as (32), i.e. approximately \( L \) times more insertions \( \gamma \) than deletions \( \delta \) can be tolerated. From (32) we also see that a good list decoder for interleaved KK subspace codes should return on average a list of size close to one if \( \gamma \) and \( \delta \) satisfy (32). This observation motivates to consider the list decoder as a probabilistic unique decoder.

4.2. Probabilistic Unique Decoder. This decoding principle can also be used as a probabilistic unique decoder. We obtain a unique solution to the root-finding problem (27) if the rank of \( Q \) is full. If \( Q \) does not have full rank, we declare a decoding failure and call the occurred error non-correctable. In the following, we show that under certain conditions the probability of a non-correctable error is very small.

Lemma 4.3. The root-finding system (27) has a unique solution if and only if \(|\mathcal{G}_{<D}| = L\).

Proof. If we set up \( Q \) using \( \mathcal{G}_{<D} \) then by Lemma 3.9 the root-finding matrix \( Q \) has full rank if \(|\mathcal{G}_{<D}| = L\). By Lemma 3.7 we always have \( 1 \leq |\mathcal{G}_{<D}| \leq L \). Let \( d_I \) be the dimension of the solution space of (13). Now assume that \(|\mathcal{G}_{<D}| < L \) and suppose that there exist \( d_I \geq L \) polynomials \( \hat{Q}^{(1)}, \ldots, \hat{Q}^{(d_I)} \in \mathbb{K}_{n_r} \) with \( \deg_{\mathbb{K}}(\hat{Q}^{(j)}) < D \) for all \( j \in [1, d_I] \) such that

\[
\hat{Q}^{(j)} \left( x, f^{(1)}(x), \ldots, f^{(L)}(x) \right) = 0, \forall j \in [1, d_I]
\]

has a unique solution. The polynomials \( \hat{Q}^{(j)} \) can be generated by \( \mathbb{L}_{eq}[x] \)-linear combinations of the elements in \( \mathcal{G}_{<D} = \{ Q^{(1)}, \ldots, Q^{(|\mathcal{G}_{<D}|)} \} \), i.e.

\[
\hat{Q}^{(j)} = \sum_{\ell=1}^{(|\mathcal{G}_{<D}|)} a^{(j)}_{\ell}(x) \otimes Q^{(\ell)}
\]

(34)
for some $a^{(j)}_\ell \in \mathbb{F}_q$ not all zero. From (34) we see that $\hat{Q}^{(j)}(x, f^{(1)}(x), \ldots, f^{(L)}(x)) = 0$ for all solutions $f^{(1)}(x), \ldots, f^{(L)}(x)$ of $Q^{(j)}(x, f^{(1)}(x), \ldots, f^{(L)}(x)) = 0$ for all $\ell \in [1, |\mathcal{G}|]$ and $j \in [1, d_I]$. Since the root-finding system set up with $\mathcal{G} < D$ cannot have a unique solution if $|\mathcal{G}| < L$ there must exist a polynomial $\hat{Q}^{(j)}$ for some $j \in [1, d_I]$ that is not of the form (34) which contradicts that $\mathcal{G} < D$ is a minimal Gröbner basis for $K_{n_r} \cap \mathbb{F}_q[x, y_1, \ldots, y_L] < D$ (see Lemma 3.8).

Lemma 4.3 shows that if the root-finding system has a unique solution, a minimal Gröbner basis for $K_{n_r}$ suffices to find this unique solution. Lemma 4.3 also implies that we may get a unique solution only if for the matrix $R$ from (13) it holds that

$$d_I \overset{\text{def}}{=} \dim \ker(R) \geq L. \quad (35)$$

We now derive a degree constraint $D_u \geq D$ which ensures that $d_I \geq L$.

**Lemma 4.4 (Degree Constraint for Probabilistic-Unique Decoding).** Let the degree constraint in Problem 1 be

$$D_u = \left\lceil \frac{n_r + \hat{k}}{L+1} \right\rceil. \quad (36)$$

Then the dimension $d_I$ of the solution space of (13) satisfies $d_I \geq L$.

**Proof.** The dimension $d_I$ of the solution space of (13) is

$$d_I = D_u(L + 1) - \hat{k} + L - \text{rk}(R)$$

where $\text{rk}(R) \leq n_r$. In order to satisfy (35) we require

$$d_I \geq D_u(L + 1) - \hat{k} + L - n_r \geq L$$

and get

$$D_u \geq \frac{n_r + \hat{k}}{L+1}.$$ 

Hence, the choice of $D_u$ in (36) ensures that $d_I \geq L$. \qed

Lemma 4.4 provides the degree constraint $D_u$ for the unique decoder to obtain the set $\mathcal{G} < D = D_u$. Since Lemma 4.3 holds in both directions we know that at least one of the $L$ polynomials $g_1, \ldots, g_L \in \mathcal{G}$ violates the degree constraint $D_u$ if there is no unique solution, i.e. $|\mathcal{G} < D| < L$ for $D = D_u$. Thus, we declare a decoding failure if at least one polynomial of $g_1, \ldots, g_L \in \mathcal{G}$ has $w$-weighted degree at least $D_u$.

Compared to the matrix-based approach in [39] the detection of decoding failures is more efficient since computing the rank of a $d_I \times L$ matrix needs more operations than determining the degree of a linearized polynomial.

To recover the message polynomials $f^{(1)}(x), \ldots, f^{(L)}(x)$, (19) has to be satisfied for all sets of $L$ polynomials that are a solution of Problem 1 with $D = D_u$. This is true if $D_u$ is less than or equal to the number of linearly independent interpolation points, i.e. if

$$D_u \leq n_t - \delta \iff \left\lceil \frac{n_r + \hat{k}}{L+1} \right\rceil \leq n_t - \delta \quad (37)$$

$$\iff \gamma + L\delta \leq L n_t - \hat{k}.$$
Notice that \( \lceil \frac{n_r + \hat{k}}{L + 1} \rceil \geq \frac{n_r + \hat{k}}{L + 1} \) and we therefore use the lower bound in (37) as it gives the largest decoding region.

For a homogeneous interleaved KK subspace code \( C_s = \text{ISub}[L, a; n_t, k] \) the probabilistic unique decoding region (37) is

\[
\gamma + L\delta \leq L(n_t - k) = L \left( \frac{d_s(C_s) - 2}{2} \right)
\]

\[\iff\]

\[
\gamma + L\delta < L \left( \frac{d_s(C_s)}{2} \right) - (L - 1).
\]

Compared to the decoding region of the list decoder (18), the ability for probabilistic unique decoding (37) comes with a penalty of \( (L - 1) \) on the decoding region.

The decoding region (38) shows a similar asymmetry between insertions and deletions as the decoding region that we derived from the average list size of homogeneous interleaved KK subspace codes (32).

Figure 2 shows the improvement of the decoding region for the probabilistic unique decoder (38) upon Kötter-Kschischang codes \( (L = 1) \) due to interleaving. Compared to the decoding region of the list decoder in Figure 1 we see that the number of correctable insertions of the probabilistic unique decoder is decreased by \( (L - 1) \).

We now upper bound the decoding failure probability using results from [39].

**Lemma 4.5** (Fraction of Non-Correctable Errors). Let \( d_l \geq L \) (see (35)) and \( |G_{<D}| = L \). Let \( Q \) be as in (26), and let \( q_{L,0}^{(\ell)}, \ldots, q_{L,0}^{(\ell)} \), for \( \ell \in [1, L] \) be random elements uniformly distributed over \( \mathbb{F}_{q^m} \). Then the fraction of non-correctable errors is upper bounded by

\[
P(|G_{<D}| < L) = P(\text{rk}(Q) < Lk) \leq 4q^{-(m(d_l + 1 - L))}.
\]

**Proof.** Lemma 4.3 shows that there exists a unique solution to the root-finding system (27) if and only if \( |G_{<D}| = L \) implying that \( \Pr[|G_{<D}| < L] = \Pr[\text{rk}_{q}(Q) < Lk] \).

It was shown in [39, Lemma 9] that under the assumption that the coefficients
Let the minimal number of insertions $\gamma$ and deletions $\delta$ that are needed to get from a codeword of $C_a = \text{ISub}[L; \mathbf{a}; n_t, k^{(1)}, \ldots, k^{(L)}]$ to the received subspace fulfill (37). Then, given the received subspace, the unique probabilistic decoder will return the original codeword with probability at least

$$1 - 4q^{-\left(m\left(L\left[\frac{n_t+\hat{k}}{L+1}\right]-\hat{k}-\gamma+1\right)\right)}.$$
4.3. Simulation results. In a simulation with $10^6$ transmissions over an operator channel with $\delta = 0$, $\gamma = 5$ and code parameters $q = 2$, $m = 8$, $n_t = 7$, $k^{(1)} = k^{(2)} = 4$, $L = 2$, we observed a fraction of $1.5 \cdot 10^{-5}$ non-correctable errors (upper bound $6.1 \cdot 10^{-5}$).

We simulated a code with parameters $m = n_t = 6$, $k = 2$ and $L = 2$ over an operator channel with $\gamma = 2, \ldots, 8$ and $\delta = 0, 1$. The results are shown in Table 1 and illustrated in Figure 3.

4.4. Error-correction with the complementary code. Consider an $L$-interleaved KK subspace code $C_s = \text{ISub}[L, n_t, k^{(1)}, \ldots, k^{(L)}]$. Suppose we transmit $V^\perp \in C_s^\perp$ and $\delta$ deletions and $\gamma$ insertions occur in the channel which outputs then
$U^\perp$. At the receiver we calculate the dual space $U$ of the received space $U^\perp$, which is shown to be a codeword from $C_s$ which is corrupted by $\delta$ insertions and $\gamma$ deletions, i.e., an insertion into $U^\perp$ becomes a deletion in $U$ and vice versa. We can then perform decoding with the known interleaved decoding algorithms in the code $C_s$.

**Lemma 4.8.** We have

$$\left(\mathcal{H}_{N-n_t-\delta}(V^\perp)\right)^\perp = V \oplus \mathcal{E}_\delta$$

for some subspace $\mathcal{E}_\delta$ of dimension $\delta$.

**Proof.** Clearly, $\mathcal{H}_{N-n_t-\delta}(V^\perp) \subseteq V^\perp$ and therefore,

$$V \subseteq \left(\mathcal{H}_{N-n_t-\delta}(V^\perp)\right)^\perp.$$ 

Further, $\dim(\mathcal{H}_{N-n_t-\delta}(V^\perp)) = N - n_t - \delta$ and thus $\dim\left(\mathcal{H}_{N-n_t-\delta}(V^\perp)^\perp\right) = n_t + \delta$.

Thus, $\left(\mathcal{H}_{N-n_t-\delta}(V^\perp)^\perp\right)$ can be decomposed as a direct sum of $V$ and some space of dimension $\delta$, which is denoted by $\mathcal{E}_\delta$.

Then, we obtain the following statement for the error-correction capability of $C_s^\perp$.

**Theorem 4.9.** Given the output of the operator channel $U^\perp = \mathcal{H}_{N-n_t-\delta}(V^\perp) \oplus \mathcal{E}_\gamma$, where $V^\perp \in C_s^\perp$ and $\dim(\mathcal{E}_\gamma) = \gamma$. If

$$\delta + L\gamma \leq L\left(\frac{d_s(C_s) - 2}{2}\right),$$

then we can reconstruct $V^\perp$ with probability at least

$$1 - 4^{-m\left(\left\lfloor \frac{N - \dim(V^\perp) - \gamma + \delta + \delta}{k - 1}\right\rfloor - k - \delta + 1\right)}.$$ 

**Proof.** We obtain:

$$U = (U^\perp)^\perp = (\mathcal{H}_{N-n_t-\delta}(V^\perp) \oplus \mathcal{E}_\gamma)^\perp = (\mathcal{H}_{N-n_t-\delta}(V^\perp)^\perp \cap \mathcal{E}_\gamma^\perp) = (V \oplus \mathcal{E}_\delta) \cap \mathcal{E}_\gamma^\perp = (V \cap \mathcal{E}_\gamma^\perp) \oplus \mathcal{E}_\delta = \mathcal{H}_{n_t-\gamma}(V) \oplus \mathcal{E}_\delta$$

where the third line follows by Lemma 4.8 and the fourth step follows since $\mathcal{E}_\delta \cap \mathcal{E}_\gamma^\perp = \mathcal{E}_\delta$. From the operator channel we have

$$V^\perp \cap \mathcal{E}_\gamma = 0 \quad \Rightarrow \quad V^\perp \subseteq \mathcal{E}_\gamma^\perp$$

since $V^\perp \oplus V = F_q^N$ and $\dim(V^\perp) \leq \dim(\mathcal{E}_\gamma^\perp)$. From Lemma 4.8 we have

$$V \cap \mathcal{E}_\delta = 0 \quad \Rightarrow \quad \mathcal{E}_\delta \subseteq V^\perp.$$

Hence, $\mathcal{E}_\delta \subseteq V^\perp \subseteq \mathcal{E}_\gamma^\perp$.

The fifth step follows because $\dim(\mathcal{E}_\gamma^\perp) = N - \gamma$ which therefore deletes exactly $\gamma$ dimensions of $V$ since $\dim(U) = N - \dim(U^\perp) = \dim(V) - \gamma + \delta$.

Thus the received space $U$ corresponds to a codeword $V \in C_s$ that is corrupted by at most $\gamma$ deletions and $\delta$ insertions. Due to (38), we can reconstruct $V$ if $L\gamma + \delta \leq L(d_s(C_s) - 2)/2$ with high probability. Once we have $V$, we can simply calculate the dual space and get $V^\perp$. 

Decoding of Interleaved Subspace and Gabidulin Codes Using Gröbner Bases 793

Advances in Mathematics of Communications Volume 12, No. 4 (2018), 773–804
The asymmetry between correcting deletions and insertions therefore flips compared to (38). The code $C_x$ is more resilient against insertions while the complementary code $C_x^\perp$ is more resilient against deletions. Notice that the list decoder can be adapted to the complementary code in a similar way.

5. Efficient interpolation of minimal Gröbner basis polynomials

In this section, we show how the generalization [42] of the multivariate Kötter interpolation [40] and the row reduction algorithm from [27] can be used to construct an ordered minimal Gröbner basis for the left $\mathbb{L}_q[x]$-submodule $K_{n_r}$ efficiently.

5.1. General linearized Kötter interpolation. A single polynomial which is a solution to Problem 1 can be constructed efficiently by the general linearized polynomial interpolation algorithm by Xie, Yan and Suter [42], requiring at most $O(L^2 n_t D)$ operations in $\mathbb{F}_q$. Our main contribution is to show how this algorithm can be used to construct a minimal Gröbner basis for $K_{n_r}$ under $\prec_w$ efficiently.

Algorithm 1 in [42] iteratively constructs $L + 1$ polynomials $x_{i,j}$ in each step $i$ that are minimal in $T_{i,j}$ w.r.t. the $w$-weighted degree for $j \in [0, L]$. The output of the algorithm in [42] is one polynomial $Q^*$ of least weighted degree among all polynomials in $K_{n_r}$.

Instead of returning only the minimal $Q^* \in K_{n_r}$, we return $g_{n_r,0}, \ldots, g_{n_r,L}$, which are minimal in $T_{n_r,0}, \ldots, T_{n_r,L}$, respectively.

Hence we modify the algorithm so that it outputs $g_{n_r,0}, \ldots, g_{n_r,L}$ and denote this adapted version by InterpolateBasis$(\mathbf{x}^T, r^{(1)}(\cdot), \ldots, r^{(L)}(\cdot))$. The pseudo-code of InterpolateBasis$(\cdot)$ is given in Algorithm 1.

Lemma 5.1. The set $\mathcal{G} = \{g_{n_r,0}, g_{n_r,1}, \ldots, g_{n_r,L}\}$ is an ordered minimal Gröbner basis for the left $\mathbb{L}_q[x]$-submodule $K_{n_r}$ under $\prec_w$.

Proof. By [42, Lemma 2] each $g_{n_r,j} = \min \{ K_{n_r} \cap S_j \} = \min \{ T_{n_r,j} \}$ with respect to the weighted degree $\deg_w$. Imposing that $LP(g_{n_r,j}) = j$. Since $K_{n_r} = T_{n_r,0} \cup T_{n_r,1} \cup \cdots \cup T_{n_r,L}$, the polynomials $g_{n_r,0}, \ldots, g_{n_r,L}$ are a basis for the $\mathbb{L}_q[x]$-submodule $K_{n_r}$. Suppose there exists a $p \in \mathcal{G}$ such that $LT(p)$ divides $LT(g_{n_r,j})$ for $q \in \mathcal{G}$, $p \neq g_{n_r,j}$. Then $g_{n_r,j}$ can be reduced modulo $p$ resulting in a polynomial with leading position $j$ and $w$-weighted degree less than $\deg_w(g_{n_r,j})$. This contradicts the minimality of $g_{n_r,j}$ in $T_{n_r,j}$.

Since we only modify the output of [42, Algorithm 1] the construction of the minimal Gröbner basis does not require more operations than constructing one polynomial. Thus the number of required operations in $\mathbb{F}_q$ is on the order of $O(L^2 n_t D)$ (see [42]). Since $D \leq n_t$ we have $O(L^2 n_t D) \leq O(L^2 n_r^2)$.

This interpretation of [42] can be directly applied to the decoding approach for interleaved Gabidulin codes in [39]. Fig. 4 shows the number of multiplications needed for efficient interpolation and compares this to the number of multiplications needed to solve (14) by Gaussian elimination. The figure shows that our interpolation-based decoding substantially reduces complexity for large $n_t$.

6. Efficient root-finding

In [39] it was shown that the root-finding system (27) can be solved recursively with at most $O(L^3 K^2)$ operations in $\mathbb{F}_q$. In this section, we present an efficient root-finding algorithm for the probabilistic unique decoder that finds all roots $f^{(1)}(x)$, $j \in \mathbb{F}_q$. The algorithm is based on a probabilistic reduction to the list decoder and consists of several steps: (1) Compute the set of all roots of $f^{(1)}(x)$ for each $j$. (2) Interpolate the roots of $f^{(1)}(x)$ for each $j$ using the general linearized Kötter interpolation. (3) Compute the list decoder for each $f^{(1)}(x)$ and output the roots of $f^{(1)}(x)$ that are closest to the root set.

Since the number of required operations in $\mathbb{F}_q$ is on the order of $O(L^3 K^2)$ we have a complexity of $O(L^3 K^2)$ for the root-finding algorithm.
Algorithm 1: Adapted Linearized Polynomial Interpolation by [42]

InterpolateBasis($x^T, r^{(1)}_i, \ldots, r^{(L)}_i$)

\textbf{Input:} A basis for the received subspace $(x_i, r^{(1)}_i, \ldots, r^{(L)}_i), i \in [0, n_r - 1]$

\textbf{Output:} An ordered minimal Gröbner basis $G = \{g_{n_r,0}, \ldots, g_{n_r,L}\}$ for $K_{n_r}$ under $\prec_w$

1 \textbf{Initialize:} $g_{0,0} = x, g_{0,j} = y_j, j \in [1, L]$

2 \textbf{Define:} $F_i(g_{i,j}) = g_{i,j}(x, r^{(1)}_i, \ldots, r^{(L)}_i)$

3 for $i \leftarrow 0$ to $n_r - 1$

4 \hspace{1em} for $j \leftarrow 0$ to $L$

5 \hspace{2em} $g_{i+1,j} \leftarrow g_{i,j}$

6 \hspace{2em} $\Delta_{i,j} \leftarrow F_i(g_{i,j})$

7 \hspace{2em} $J \leftarrow \{j : \Delta_{i,j} \neq 0\}$

8 \hspace{2em} if $J \neq \emptyset$

9 \hspace{3em} $j^* \leftarrow \min \{\min_{j \in J} \{\deg_w(g_{i,j})\}\}$

10 \hspace{3em} for $j \in J$

11 \hspace{4em} if $j \neq j^*$ then

12 \hspace{5em} $g_{i+1,j} \leftarrow \Delta_{i,j} \cdot g_{i,j} - \Delta_{i,j} g_{i,j^*}$

13 \hspace{4em} else if $j = j^*$ then

14 \hspace{5em} $g_{i+1,j} \leftarrow \Delta_{i,j} \cdot (x^{[1]} \otimes g_{i,j^*}) - F_i(x^{[1]} \otimes g_{i,j^*}) g_{i,j^*}$

15 \hspace{2em} return $G = \{g_{n_r,0}, \ldots, g_{n_r,L}\}$

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure4.png}
\caption{Multiplications vs. the number of insertions for $L = 4$.}
\end{figure}
An efficient root-finding algorithm. Let $\mathcal{G} = \{g_0, g_1, \ldots, g_L\}$ be an ordered minimal Gröbner basis under $\prec_w$ for the left $L_{q^m}[x]$-submodule $\mathcal{K}_n$. Suppose that all polynomials in $\mathcal{G}$ except $g_0$ (see Lemma 3.7) have weighted degree less than $D_u$, i.e., $|\mathcal{G}_{<D}| = L$. Since $\mathcal{G}$ is a minimal Gröbner basis the polynomials in $\mathcal{G}_{<D}$ have distinct leading positions. This property imposes a triangular structure on the linear root-finding system (27) and allows to solve it efficiently. In particular, we can solve the upper-triangular subsystem (28) for the case where $|\mathcal{G}_{<D}| = L$ since we know from Lemma 3.9 that this system has full rank. Thus, using an ordered minimal Gröbner basis allows to reduce the complexity of the root-finding step.

If $|\mathcal{G}_{<D}| = L$, Algorithm 2 recursively determines all unique roots $f_j^{(j)}(x)$, $j \in [1, L]$. Algorithm 2 is based on the symbolic right division of univariate linearized polynomials and solves the root-finding system recursively.

**Algorithm 2:** Unique root-finding of $y_1, \ldots, y_L$-minimal polynomials $f_1^{(1)}(x), \ldots, f_L^{(1)}(x) \leftarrow \text{findRoots}(g_1, \ldots, g_L, k^{(1)}, \ldots, k^{(L)})$

input: $\mathcal{G}_{<D} = \{g_1, \ldots, g_L\}$ with $\mathcal{L}(g_j) = j, \forall j \in [1, L]$  
output: L unique linearized message polynomials $f_1^{(1)}(x), \ldots, f_L^{(1)}(x)$,  
$\deg_q(f_j^{(j)}(x)) < k^{(j)}$ for $j \in [1, L]$

1 for $i \leftarrow 1$ to $\max_{j \in [1, L]} \{k^{(j)}\}$ do
2 for $j \leftarrow 1$ to $L$ do
3 $b \leftarrow \deg_q(Q_0^{(0)}(x)), e \leftarrow \deg_q(Q_j^{(j)}(y_j))$
4 if $b - e = k^{(j)} - i$ and $b - e \geq 0$ then
5 $t_i^{(j)}(x) \leftarrow -\frac{LC(Q_0^{(0)}(x))}{LC(Q_j^{(j)}(y_j))} x^{[m-e]}$
6 $f_j^{(j)}(x) \leftarrow f_j^{(j)}(x) + t_i^{(j)}(x)$
7 for $\ell \leftarrow i$ to $L$ do
8 $Q_0^{(0)}(x) \leftarrow Q_0^{(0)}(x) + Q_j^{(j)}(x) \otimes t_i^{(j)}(x)$

**Theorem 6.1 (Correctness of Algorithm 2).** Let $\mathcal{G}_{<D} = \{Q_1^{(1)}, \ldots, Q_L^{(L)}\}$ be a subset of an ordered minimal Gröbner basis of $\mathcal{G}_n$, with $LT(Q_j^{(j)}) = j, \forall j \in [1, L]$. Then, for all $j \in [1, L]$, Algorithm 2 determines the unique polynomials $f_j^{(j)}(x) = \sum_{i=0}^{k^{(j)}} f_i^{(j)}(x)$ such that

$$P^{(j)}(x) \overset{\text{def}}{=} Q_0^{(0)}(x) + Q_1^{(1)}(f^{(1)}(x)) + \cdots + Q_l^{(l)}(f^{(L)}(x)) = 0.$$  

Proof. Let $b = \deg_q(Q_0^{(0)}(x))$ and $e = \deg_q(Q_j^{(j)}(y_j))$. The polynomial $Q_j^{(j)}(x, y_1, \ldots, y_L)$ is $y_j$-minimal for any $j \in [1, L]$ and thus the $q$-degrees fulfill $b \leq e + k^{(j)} - 1$ and $\deg_q(Q_j^{(j)}(y_j)) < e$ for $j' > j$. This implies that the coefficients are $q_{j', e}^{(j)} = 0$ for $j' > j$. In the first iteration $j = i = 1$ we must solve $\sum_{\ell=1}^{L} q_{\ell, e}^{(1)} \cdot f_\ell^{(1)}(x) x^{[k^{(\ell)}+e-1]} = -q_{0, b}^{(1)}$. Since $q_{1, e}^{(1)} = 0$ for $\ell \in [2, L]$ the calculation reduces to
\( q_{1,e} \cdot f_{k^{(1)}-1}^{(1)}x^{[k^{(1)}+e-1]} = -q_{0,b}^{(1)}x^{[b]} \). Hence, the monomial \( t_1^{(1)}(x) = f_{k^{(1)}-1}^{(1)}x^{[k^{(1)}-1]} \) can uniquely be determined as

\[
\tag{43}
f_{k^{(1)}-1}^{(1)}x^{[k^{(1)}-1]} = \left( -\frac{q_{0,b}^{(1)}}{q_{1,e}^{(1)}} \right) [m-e] x^{[b-e]}.
\]

which corresponds to line 5 in Algorithm 2 and it is easy to check that

\[
\tag{44}
\text{LT}(Q_1^{(1)}(y_1) \otimes t_1^{(1)}(x)) = q_{1,e}^{(1)} \cdot (t_1^{(1)}(x))^{[e]}
\]

\[
= q_{1,e}^{(1)} \cdot \left( -\frac{q_{0,b}^{(1)}}{q_{1,e}^{(1)}} [m-e] x^{[b-e]} \right)^{[e]} = -q_{0,b}^{(1)}x^{[b]}.
\]

If \( b - e < k^{(1)} - 1 \), then \( f_{k^{(1)}-1}^{(1)} \) has to be zero to ensure \( q_{1,e}^{(1)} \cdot f_{k^{(1)}-1}^{(1)}x^{[k^{(1)}+e-1]} = -q_{0,b}^{(1)} \), i.e., no update on \( f_{k^{(1)}-1}^{(1)} \) is done. Now \( Q_0^{(2)}(x), \forall \ell \in [1, L] \) are updated with

\[
Q_0^{(2)}(x) = Q_0^{(2)}(x) + Q_1^{(1)}(x) \otimes t_1^{(1)}(x).
\]

which reduces the \( q \)-degree of \( Q_0^{(1)}(x) \) by one since we enforced (44).

In the next iteration \( i = 1, j = 2 \) we must solve \( \sum_{\ell=1}^{L} q_{\ell,e}^{(2)} \cdot f_{k^{(2)}-1}^{(2)}x^{[k^{(2)}+\ell-1]} = -q_{0,b}^{(2)}x^{[b]} \) which reduces to

\[
\sum_{\ell=1}^{2} q_{\ell,e}^{(2)} \cdot f_{k^{(2)}-1}^{(2)}x^{[k^{(2)}+\ell-1]} = -q_{0,b}^{(2)}x^{[b]}
\]

\[
\equiv q_{2,e}^{(2)} \cdot f_{k^{(2)}-1}^{(2)}x^{[k^{(2)}+e-1]} = -\left( q_{0,b}^{(2)}x^{[b]} + q_{1,e}^{(2)} \cdot f_{k^{(2)}-1}^{(2)}x^{[k^{(2)}+\ell-1]} \right)
\]

\[
\equiv q_{2,e}^{(2)} \cdot f_{k^{(2)}-1}^{(2)}x^{[k^{(2)}+\ell-1]} = -q_{0,b}^{(2)}x^{[b]}
\]

due to the \( y_2 \)-minimality of \( Q_2^{(2)}(x, y_1, \ldots, y_s) \). Hence, we can directly calculate the coefficient \( f_{k^{(2)}-1}^{(2)} \) using the updated polynomial \( Q_0^{(2)}(x) \) from the previous step.

The algorithm computes the unique monomial \( f_{k^{(2)}-1}^{(2)}x^{[k^{(2)}-1]} \) in each step \( i, j \) such that

\[
q_{j,e}^{(1)} \cdot f_{k^{(2)}-1}^{(2)}x^{[k^{(2)}+\ell-1]} = -\left( q_{0,b}^{(1)}x^{[b]} + \sum_{\ell=1}^{j-1} q_{\ell,e}^{(1)} \cdot f_{k^{(2)}-1}^{(2)}x^{[k^{(2)}+\ell-1]} \right)
\]

which is possible since the right hand side is computed in step \( i, j - 1 \) of Algorithm 2.

\[ Q_0^{(2)}(x) = Q_0^{(2)}(x) + Q_1^{(1)}(x) \otimes t_1^{(1)}(x). \]

6.2. Complexity Analysis. Suppose we use a normal basis (which always exists). The calculation of \( q \)-powers then corresponds to a cyclic shift over the base field and its complexity can be neglected. Hence, multiplications dominate the complexity.

**Lemma 6.2** (Complexity of the Root-Finding Algorithm). Let \( Q^{(j)} \in L_{q^m}[x, y_1, \ldots, y_L] \) be \( y_j \)-minimal and let \( \deg_w(Q^{(j)}) < D, \forall j \in [1, L] \). Then the \( L \) unique message polynomials \( f^{(j)}(x), j \in [1, L], \) such that

\[
P(x) = Q^{(j)} \left( x, f^{(1)}(x), \ldots, f^{(L)}(x) \right) = 0
\]

can be found with \( \mathcal{O}(L^2k^2) \) operations in \( \mathbb{F}_{q^m} \).
Proof. Each step of Algorithm 2 provides \( L \) compositions of a (univariate) linearized polynomial of \( q \)-degree at most \( D - k \) with one monomial. If we consider the inversion of an element from \( \mathbb{F}_{q^m} \) as a multiplication we have \( L(D - k + 2) \) multiplications per step. In total we need \( kL^2(D - k + 2) \leq k^2L^2 \) multiplications in \( \mathbb{F}_{q^m} \).

A comparison of this complexity to the recursive Gaussian elimination (GE) from [39] is illustrated in Figure 5.

![Figure 5](image_url)  
**Figure 5.** Number of multiplications for root-finding step for different interleaving orders \( L \). The complexity of the recursive GE is independent of \( \gamma \).

Besides the reduction in computational cost, Algorithm 2 requires less memory than the recursive GE. An upper bound on the memory requirement is given by the following lemma.

**Lemma 6.3 (Memory Requirement of Algorithm 2).** Let \( k = \max_{j \in [1, L]} \{k^{(j)}\} \). The memory requirement of Algorithm 2 is upper bounded by \( L^2(D - k + 1) + L(D + k) \).

**Proof.** The algorithm must store \( L \) \((L + 1)\)-variate polynomials with each at most \( D(L + 1) - L(k - 1) \) coefficients in \( \mathbb{F}_{q^m} \), as well as the \( Lk \) coefficients in \( \mathbb{F}_{q^m} \) of the \( L \) message polynomials. Hence, in total we must store \( L^2(D - k + 1) + L(D + k) \) elements in \( \mathbb{F}_{q^m} \).

The memory requirements of Algorithm 2 and the recursive GE are illustrated in Figure 6.

### 7. Efficient Decoding Algorithm

We now summarize the efficient decoding procedure for list and probabilistic unique decoding of interleaved KK subspace and Gabidulin codes.
Figure 6. Memory requirements of the root-finding step for $n_t = 80$, $k = 60$

**Theorem 7.1 (List Decoding of Interleaved KK Codes).** Consider an $L$-interleaved subspace code $\text{ISub}[L, a; n_t, k(1), \ldots, k(L)]$. Let $\hat{k} = \sum_{j=1}^{L} k(j)$. Let the number of insertions $\gamma$ and deletions $\delta$ satisfy

$$\gamma + L\delta < L(n_t + 1) - \hat{k}.$$ 

Then a list $\mathcal{L}$ of size

$$|\mathcal{L}| \leq q^{m\left(k - \min_{j \in [1, L]} \{k(j)\}\right)}$$

containing all tuples of message polynomials $(f(1)(x), \ldots, f(L)(x))$ that correspond to codewords in subspace distance at most $\gamma + \delta$ from the received space can be obtained requiring at most $O(L^2 n_r^2)$ operations in $\mathbb{F}_{q^m}$.

**Proof.** The decoding region follows from Theorem 3.3 and the maximum list size follows from Lemma 4.1. The required minimal Gröbner basis for the interpolation module $\mathcal{K}_{n_r}$ can be constructed using Algorithm 1 in at most $O(L^2 n_r^2)$ operations in $\mathbb{F}_{q^m}$.

**Theorem 7.2 (Unique Decoding of Interleaved Subspace Codes).** Consider an $L$-interleaved KK subspace code $\text{ISub}[L, a; n_t, k^{(1)}, \ldots, k^{(L)}]$. Let $\hat{k} = \sum_{j=1}^{L} k^{(j)}$. Let the number of insertions $\gamma$ and deletions $\delta$ satisfy

$$\gamma + L\delta \leq L n_t - \hat{k}.$$ 

Then the unique tuple $(f(1)(x), \ldots, f(L)(x))$ containing the linearized message polynomials $f^{(j)}(x) \in \mathbb{L}_{q^m}[x]_{<k^{(j)}}$ for all $j \in [1, L]$ that satisfy (19) can be found with probability at least

$$1 - 4q^{-m\left(L\lceil \frac{\gamma + \delta}{L}\rceil - \hat{k} - \gamma + 1\right)}$$

requiring at most $O(L^2 n_r^2)$ operations in $\mathbb{F}_{q^m}$.
The decoding procedure uses the efficient interpolation and root-finding algorithm for list decoding of KK codes and is summarized in Algorithm 3. By Theorem 3.10 the list size can be upper bounded from the set of leading positions \( \mathcal{J} = \text{LP}(\mathcal{G} \setminus \mathcal{G}_D) \). Thus Algorithm 3 can be modified so that it returns a list of bounded size by computing the list size using \( \mathcal{J} \) right after the construction of \( \mathcal{G}_D \) or declare a decoding failure if the list size exceeds a fixed threshold. In order to

\[
\text{Algorithm 3: \text{ListDecodeIntSub}(x^T, r^{(1)}T, \ldots, r^{(L)}T)}
\]

\textbf{Input}: A basis \((x^T, r^{(1)}T, \ldots, r^{(L)}T)\) for the \( n_r \)-dimensional received subspace.

\textbf{Output}: A list \( \mathcal{L} \) of tuples \( (f^{(1)}(x), \ldots, f^{(L)}(x)) \)

1 \textbf{Interpolation step:}
2 \( \mathcal{G} \leftarrow \text{InterpolateBasis}(x^T, r^{(1)}T, \ldots, r^{(L)}T) \)

3 \textbf{Root-finding step:}
4 Construct the set \( \mathcal{G}_D = \{ \tilde{g} \in \mathcal{G} : \deg_w(\tilde{g}) < D \} \)
5 Set up the root-finding matrix \( \mathbf{Q} \) (26) and the vector \( \mathbf{q}_0 \) using \( \mathcal{G}_D \)
6 Determine all solutions of the root-finding system \( \mathbf{Q} \cdot \mathbf{f} = \mathbf{q}_0 \), i.e., all roots of (12)
7 \textbf{Output}: List \( \mathcal{L} \) of all tuples \( (f^{(1)}(x), \ldots, f^{(L)}(x)) \) that correspond to solutions of the root-finding system (27)

efficiently decode interleaved Gabidulin codes of length \( n \), elementary dimensions \( k^{(j)} \) and interleaving order \( L \) as defined in \([22, 30, 39]\) we set \( n_t = n_r = n \). Let \( \mathbf{g} = \{ g_0, \ldots, g_{n-1} \} \subset \mathbb{F}_{q^m} \) with \( n \leq m \) denote the linearly independent code locators of the interleaved Gabidulin code and denote by \( \mathbf{y}^{(j)}, j \in [1, L] \) the elementary received words. Then, Algorithm 3 called with \((\mathbf{g}^T, \mathbf{y}^{(1)}T, \ldots, \mathbf{y}^{(L)}T)\) can decode errors of rank \( t \) up to \( t < \frac{L(n-k+1)}{L+1} \) (see [39]).

The complete procedure for the probabilistic unique decoder for interleaved KK codes is given in Algorithm 4. To decode an interleaved Gabidulin code, this procedure must be called with \((\mathbf{g}^T, \mathbf{y}^{(1)}T, \ldots, \mathbf{y}^{(L)}T)\). As in [39], the decoder finds a unique solution with high probability for \( t \leq \frac{L(n-k)}{L+1} \).

The computational complexity of Algorithm 3 and Algorithm 4 is dominated by the interpolation and the root-finding step. Using Algorithm 1 the complexity of constructing the minimal Gröbner basis for the interpolation module is in the order of \( \mathcal{O}(L^2 n_t^2) \) operations in \( \mathbb{F}_{q^m} \). The root-finding step using Algorithm 2 requires at most \( \mathcal{O}(L^2 k^2) \) operations in \( \mathbb{F}_{q^m} \). Thus the overall computational complexity of the list and unique decoding algorithm is at most \( \mathcal{O}(L^2 n_t^2) \) operations in \( \mathbb{F}_{q^m} \) where \( k = \max_{j \in [1, L]} \{ k^{(j)} \} \). Similar to previous work [18], we count operations in \( \mathbb{F}_{q^m} \), i.e., this includes multiplications, additions, and inversions.

\section*{8. Comparison to known decoding schemes}

It has been shown that decoding KK subspace codes can be transformed to a generalized rank-metric decoding problem [33]. The main idea of this approach is to use information from the channel to decode a codeword of an interleaved Gabidulin
express \( \gamma \) \( \mathbb{K} \) subspace codes. In terms of row/column erasures and full rank errors we can decoder from Section 4 is then for all \( j \) code that is corrupted by \( \rho \) row erasures, \( \varkappa \) column erasures and \( t \) full rank errors.

A full rank error \( t \) is a deletion and an insertion at the same location (i.e. same code locator \( \alpha_i \)). Column erasures correspond to deletions at locations where no insertion occurred and row erasures correspond to insertions at positions where no deletion occurred. For comparison we only consider the homogeneous case \( k^{(j)} = k \) for all \( j \in [1, L] \) since the scheme in [15] only can construct homogeneous interleaved \( \mathbb{K} \) subspace codes. In terms of row/column erasures and full rank errors we can express \( \gamma = \varkappa + t \) and \( \delta = \rho + t \). The decoding region for the probabilistic unique decoder from Section 4 is then

\[
\varkappa + t + L(\rho + t) \leq L(n_t - k) \\
\Leftrightarrow (L + 1)t + \varkappa + L\rho \leq L(n_t - k).
\]

The decoding regions and computational decoding complexity for known unique decoding schemes are compared in Table 2.

Recall that the interleaving order \( L \) depends on the code rate \( R \) (see (10)). Further, the impact of \( L \) on the decoding performance is quite large in practice. Thus we include \( L \) in the \( O \)-notation of the computational complexity analysis. For a detailed discussion whether to include \( L \) in the \( O \)-notation we refer to [25, Chapter 1.2].

Table 2 shows that the rank-metric based decoding schemes [15,20,31] can correct more full errors with increasing \( L \) while the performance for insertions and deletions remains the same as for non-interleaved codes [18,33].

### Table 2

| Decoding scheme          | Decoding region | Op. in \( \mathbb{F}_q^n \) |
|--------------------------|-----------------|-------------------------------|
| Li–Sidorenko–Silva [20,31] | \((L + 1)t + L\varkappa + L\rho \leq L(n_t - k)\) | \(O(Ln_t^2)\) |
| Wachter-Zeh–Zeh [39]     | \((L + 1)t + L\varkappa + L\rho \leq L(n_t - k)\) | \(O(L^3n_t^2)\) |
| Guruswami–Xing [15]      | \((L + 1)t + \varkappa + L\rho \leq L(n_t - k)\) | \(O(L^3n_t^2)\) |
| Bartz–Meier–Sidorenko [4] | \((L + 1)t + \varkappa + L\rho \leq L(n_t - k)\) | \(O(L^4n_t^2)\) |
| This contribution        | \((L + 1)t + \varkappa + L\rho \leq L(n_t - k)\) | \(O(L^4n_t^2)\) |

A full rank error \( t \) is a deletion and an insertion at the same location (i.e. same code locator \( \alpha_i \)). Column erasures correspond to deletions at locations where no insertion occurred and row erasures correspond to insertions at positions where no deletion occurred. For comparison we only consider the homogeneous case \( k^{(j)} = k \) for all \( j \in [1, L] \) since the scheme in [15] only can construct homogeneous interleaved \( \mathbb{K} \) subspace codes. In terms of row/column erasures and full rank errors we can express \( \gamma = \varkappa + t \) and \( \delta = \rho + t \). The decoding region for the probabilistic unique decoder from Section 4 is then

\[
\varkappa + t + L(\rho + t) \leq L(n_t - k) \\
\Leftrightarrow (L + 1)t + \varkappa + L\rho \leq L(n_t - k).
\]

The decoding regions and computational decoding complexity for known unique decoding schemes are compared in Table 2.

Recall that the interleaving order \( L \) depends on the code rate \( R \) (see (10)). Further, the impact of \( L \) on the decoding performance is quite large in practice. Thus we include \( L \) in the \( O \)-notation of the computational complexity analysis. For a detailed discussion whether to include \( L \) in the \( O \)-notation we refer to [25, Chapter 1.2].

Table 2 shows that the rank-metric based decoding schemes [15,20,31] can correct more full errors with increasing \( L \) while the performance for insertions and deletions remains the same as for non-interleaved codes [18,33].
The interpolation-based decoding schemes from Section 4 and [15] can correct the same number of full errors as the rank-metric based schemes [15, 20, 31] but can correct $L$-times more insertions.

The codes in [15] over the field $\mathbb{F}_{q^L}$ with code locators from $\mathbb{F}_{q^m}$ are homogeneous $L$-interleaved KK subspace codes over $\mathbb{F}_{q^m}$ [6]. In this scheme all operations are performed in the larger field $\mathbb{F}_{q^L}$ which requires higher computational complexity ($\leq O(L^4n_t^2) \approx O(L^6n_t^2)$ operations in $\mathbb{F}_{q^m}$).

The syndrome-based scheme in [4] achieves the same decoding region as the proposed interpolation-based decoder from Section 4 requiring at most $O(L^3n_t^3)$ operations in $\mathbb{F}_{q^m}$. In the worst case we have $\gamma \leq Ln_t$ and thus the computational complexity of the interpolation-based scheme is in the order of $O(L^2n_t^2) < O(L^4n_t^2)$ operations in $\mathbb{F}_{q^m}$.

The proposed interpolation-based decoding scheme therefore achieves the so far best-known decoding region with significantly lower complexity than [15] and lower computational complexity than [4] for $n_t > L$. The upper bound on the failure probability is roughly $4q^{-m}$ for all schemes.

9. Conclusion

An interpolation-based decoding scheme for interleaved KK subspace codes has been presented. We have shown that interleaved subspace codes can be made more resilient against insertions as compared to the approach from [18]. Our principle can be used as a (not necessarily polynomial-time) list decoder as well as a probabilistic unique decoder. In both cases, the procedure consists of interpolating a minimal Gröbner basis for the interpolation module followed by a root-finding step.

Two procedures for efficiently constructing required minimal Gröbner basis polynomials were proposed. The procedures are based on the general linearized Kötter interpolation and row reduction in modules. Further, a computationally- and memory-efficient root-finding algorithm for the unique decoder was presented, which exploits the structure of the minimal Gröbner basis.

The results and algorithms can also be used to accelerate interpolation-based decoding for interleaved Gabidulin codes from [39].

Acknowledgments

The authors would like to thank Vladimir Sidorenko for fruitful discussions and helpful comments.

References

[1] W. W. Adams and P. Loustaunau, An Introduction to Gröbner Bases, 3, American Mathematical Soc., 1994.
[2] C. Bachoc, F. Vallentin and A. Passuello, Bounds for Projective Codes from Semidefinite Programming, Adv. Math. Commun., 7 (2013), 127–145.
[3] H. Bartz, Algebraic Decoding of Subspace and Rank-Metric Codes, PhD thesis, Technical University of Munich, 2017.
[4] H. Bartz, M. Meier and V. Sidorenko, Improved Syndrome Decoding of Interleaved Subspace Codes, in 11th International ITG Conference on Systems, Communications and Coding 2017 (SCC), Hamburg, Germany, 2017.
[5] H. Bartz and V. Sidorenko, List and probabilistic unique decoding of folded subspace codes, in IEEE International Symposium on Information Theory (ISIT), 2015.
[6] H. Bartz and V. Sidorenko, On list-decoding schemes for punctured reed-solomon, Gabidulin and subspace codes, in XV International Symposium “Problems of Redundancy in Information and Control Systems”, 2016.
[7] H. Bartz and A. Wachter-Zeh, Efficient interpolation-based decoding of interleaved subspace and Gabidulin codes, in 52nd Annual Allerton Conference on Communication, Control, and Computing, 2014, 1349–1356.

[8] D. Cox, J. Little and D. O’Shea, Ideals, Varieties, and Algorithms, vol. 3, Springer, 1992.

[9] P. Delsarte, Bilinear forms over a finite field with applications to coding theory, J. Combin. Theory, 25 (1978), 226–241.

[10] T. Etzion and N. Silberstein, Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams, IEEE Trans. Inf. Theory, 55 (2009), 2909–2919.

[11] T. Etzion and A. Vardy, Error-correcting codes in projective space, IEEE Trans. Inf. Theory, 57 (2011), 1165–1173.

[12] T. Etzion, E. Gorla, A. Ravagnani and A. Wachter-Zeh, Optimal Ferrers diagram rank-metric codes, IEEE Trans. Inform. Theory, 62 (2016), 1616–1630.

[13] E. M. Gabidulin, Theory of codes with maximum rank distance, Probl. Inf. Transm., 21 (1985), 3–16.

[14] M. Gadouleau and Z. Yan, Constant-rank codes and their connection to constant-dimension codes, IEEE Trans. Inf. Theory, 56 (2010), 3207–3216.

[15] V. Guruswami and C. Xing, List decoding Reed–Solomon, algebraic-geometric, and Gabidulin subcodes up to the singleton bound, STOC’13?Proceedings of the 2013 ACM Symposium on Theory of Computing, 843–852, ACM, New York, 2013.

[16] R. A. Horn and C. R. Johnson, Matrix Analysis, Cambridge University Press, Cambridge, 2013.

[17] A. Kohnert and S. Kurz, Construction of large constant dimension codes with a prescribed minimum distance, in Mathematical Methods in Computer Science, vol. 5393 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2008, 31–42.

[18] R. Kötter and F. R. Kschischang, Coding for errors and erasures in random network coding, IEEE Trans. Inf. Theory, 54 (2008), 3579–3591.

[19] M. Kuijper and A. Trautmann, Gröbner bases for linearized polynomials, URL http://arxiv.org/abs/1406.4600.

[20] W. Li, V. Sidorenko and D. Silva, On transform-domain error and erasure correction by Gabidulin codes, Des. Codes Cryptogr., 73 (2014), 571–586.

[21] R. Liul and H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and its Applications, Cambridge University Press, Cambridge, 1997.

[22] P. Loidreau and R. Overbeck, Decoding rank errors beyond the error correcting capability, in Int. Workshop Alg. Combin. Coding Theory (ACCT), 2006, 186–190.

[23] H. Mahdavifar and A. Vardy, Algebraic list-decoding on the operator channel, in IEEE Int. Symp. Inf. Theory (ISIT), 2010, 1193–1197.

[24] H. Mahdavifar and A. Vardy, List-Decoding of Subspace Codes and Rank-Metric Codes up to Singleton Bound, in IEEE Int. Symp. Inf. Theory (ISIT), 2012, 1488–1492.

[25] J. N. Nielsen, List Decoding of Algebraic Codes, PhD thesis, 2013.

[26] O. Ore, On a special class of polynomials, Trans. Amer. Math. Soc., 35 (1933), 559–584.

[27] S. Puchinger, J. S. R. Nielsen, W. Li and V. Sidorenko, Row reduction applied to decoding of rank metric and subspace codes, Designs, Codes and Cryptography, 82 (2017), 389–409, URL http://arxiv.org/abs/1510.04720v2.

[28] N. Raviv and A. Wachter-Zeh, Some Gabidulin codes cannot be list decoded efficiently at any radius, IEEE Trans. Inform. Theory, 62 (2016), 1605–1615.

[29] R. M. Roth, Maximum-rank array codes and their application to crisscross error correction, IEEE Trans. Inf. Theory, 37 (1991), 328–336.

[30] V. R. Sidorenko and M. Bossert, Decoding interleaved Gabidulin codes and multisequence linearized shift-register synthesis, in IEEE Int. Symp. Inf. Theory (ISIT), 2010, 1145–1152.

[31] V. R. Sidorenko, L. Jiang and M. Bossert, Skew-feedback shift-register synthesis and decoding interleaved Gabidulin codes, IEEE Trans. Inf. Theory, 57 (2011), 621–632.

[32] D. Silva, Error Control for Network Coding, PhD thesis, University of Toronto, Toronto, Canada, 2009.

[33] D. Silva, F. R. Kschischang and R. Kötter, A rank-metric approach to error control in random network coding, IEEE Trans. Inf. Theory, 54 (2008), 3951–3967.

[34] V. Skachek, Recursive code construction for random networks, IEEE Trans. Inf. Theory, 56 (2010), 1378–1382.

[35] A. L. Trautmann, F. Manganiello and J. Rosenthal, Orbit codes - A new concept in the area of network coding, in IEEE Information Theory Workshop 2019 (ITW 2019), 2010.
[36] A.-L. Trautmann and M. Kuijper, Gabidulin decoding via minimal bases of linearized polynomial modules, preprint, arXiv:1408.2303.
[37] A.-L. Trautmann, N. Silberstein and J. Rosenthal, List decoding of lifted Gabidulin codes via the Plücker embedding, in Int. Workshop Coding Cryptogr. (WCC), 2013.
[38] A. Wachter-Zeh, Bounds on list decoding of rank-metric codes, IEEE Trans. Inf. Theory, 59 (2013), 7268–7277.
[39] A. Wachter-Zeh and A. Zeh, List and unique error-erasure decoding of interleaved Gabidulin codes with interpolation techniques, Des. Codes Cryptogr., 73 (2014), 547–570.
[40] B. Wang, R. J. McEliece and K. Watanabe, Kötter interpolation over free modules, in Proc. 43rd Annu. Allerton Conf. Comm., Control, and Comp., 2005.
[41] S. Xia and F. Fu, Johnson type bounds on constant dimension codes, Des. Codes Cryptogr., 50 (2009), 163–172.
[42] H. Xie, Z. Yan and B. W. Suter, General linearized polynomial interpolation and its applications, in IEEE Int. Symp. Network Coding (Netcod), 2011, 1–4.

Received for publication February 2018.

E-mail address: hannes.bartz@dlr.de
E-mail address: antonia.wachter-zeh@tum.de