Noname manuscript No.
(will be inserted by the editor)

List Decoding of Lifted Gabidulin Codes via the Plücker Embedding

Anna-Lena Trautmann · Natalia Silberstein · Joachim Rosenthal

the date of receipt and acceptance should be inserted later

Abstract Codes in the Grassmannian have recently found an application in random network coding. All the codewords in such codes are subspaces of $\mathbb{F}_q^n$ with a given dimension.

In this paper, we consider the problem of list decoding of a certain family of codes in the Grassmannian, called lifted Gabidulin codes. For this purpose we use the Plücker embedding of the Grassmannian. We describe a way of representing a subset of the Plücker coordinates of lifted Gabidulin codes as linear block codes. The union of the parity-check equations of these block codes and the equations which arise from the description of a ball around a subspace in the Plücker coordinates describe the list of codewords with distance less than a given parameter from the received word.

1 Introduction

Let $\mathbb{F}_q$ be a finite field of size q. The *Grassmannian space* (Grassmannian, in short), denoted by $\mathcal{G}_q(k,n)$, is the set of all k-dimensional subspaces of the vector space $\mathbb{F}_q^n$, for any given two integers k and n, $0 \leq k \leq n$. A subset $\mathcal{C}$ of the Grassmannian is called an $(n,M,d_S,k)_q$ *constant dimension code* if it has size M and minimum subspace distance d_S, where the distance function in $\mathcal{G}_q(k,n)$ is defined as follows:

$$d_S(\mathcal{U},\mathcal{V}) = 2k - 2\dim\big(\mathcal{U}\cap\mathcal{V}\big), \tag{1}$$

for any two subspaces $\mathcal{U}$ and $\mathcal{V}$ in $\mathcal{G}_q(k,n)$.

These codes gained a lot of interest due to the work by Kötter and Kschischang [12], where they show the application of such codes for error-correction in random network coding. They proved that an $(n,M,d_S,k)_q$ code can correct any t packet errors (which is equivalent to t packet insertions and t packet deletions) and any τ packet erasures introduced anywhere in the network as long as $4t+2\tau < d_S$. This application has motivated extensive work in the area [1,3,4,6,7,8, 11,13,14,15,17,21,24,25]. In the same work the before mentioned authors gave a Singleton like upper bound on the size of such codes and a Reed-Solomon like code which asymptotically attains this bound. Silva, Kötter, and Kschischang [20] showed how this construction can be described in terms of lifted Gabidulin codes [5]. The generalizations of this construction and the decoding

First and third author were partially supported by Swiss National Science Foundation Grant no. 138080. The first author was partially supported by Forschungskredit of the University of Zurich, grant no. 57104103.

A.-L. Trautmann · J. Rosenthal
Institute of Mathematics, University of Zurich, Switzerland
E-mail: trautmann@math.uzh.ch, rosenthal@math.uzh.ch

N. Silberstein
Department of Electrical and Computer Engineering, University of Texas at Austin, USA
E-mail: natalys@austin.utexas.edu.

algorithms were presented in [1,3,13,17,21,25]. Another type of constructions (orbit codes) can be found in [4,11,24].

In this paper we focus on the list decoding of lifted Gabidulin codes. For the classical Gabidulin codes it was recently shown by Wachter-Zeh [26] that, if the radius of the ball around a received word is greater than the Johnson radius, no polynomial-time list decoding is possible, since the list size can be exponential. Algebraic list decoding algorithms for folded Gabidulin codes were discussed in [7,14]. The constructions of subcodes of lifted Gabidulin codes and their algebraic list decoding algorithms were presented in [8,15].

Our approach for list decoding codes in the Grassmannian is to apply the techniques of Schubert calculus over finite fields, i.e. we represent subspaces in the Grassmannian by their Plücker coordinates. It was proven in [17] that a ball of a given radius (with respect to the subspace distance) around a subspace can be described by explicit linear equations in the Plücker embedding. In this work we describe a way of representing a subset of the Plücker coordinates of lifted Gabidulin codes as linear block codes, which results in additional linear (parity-check) equations. The solutions of all these equations will constitute the resulting list of codewords.

The rest of this paper is organized as follows. In Section 2 we describe the construction of Gabidulin and lifted Gabidulin codes and discuss the Plücker embedding of subspaces in the Grassmannian. In Section 3 we describe a representation of a subset of the Plücker coordinates of a lifted Gabidulin code and present a list decoding algorithm. Conclusions and problems for future research are given in Section 4.

2 Preliminaries and Notations

We denote by GL_n the general linear group over $\mathbb{F}_q$, by S_n the symmetric group of degree n. With $\mathbb{P}^n$ we denote the projective space of order n over $\mathbb{F}_q$.

Let $p(x) = \sum p_i x^i \in \mathbb{F}_q[x]$ be a monic and irreducible polynomial of degree ℓ, and α be a root of $p(x)$. Then it holds that $\mathbb{F}_{q^\ell} \cong \mathbb{F}_q[\alpha]$. We denote the vector space isomorphism between the extension field $\mathbb{F}_{q^\ell}$ and the vector space $\mathbb{F}_q^\ell$ by

$$\begin{aligned} \phi^{(\ell)}: \quad & \mathbb{F}_{q^\ell} \longrightarrow \mathbb{F}_q^\ell \\ & \sum_{i=0}^{\ell-1} \lambda_i \alpha^i \longmapsto (\lambda_0, \ldots, \lambda_{\ell-1}). \end{aligned}$$

Moreover, we need the following notations: $\mathrm{rs}(U)$ denotes the row space of a matrix U,

$$\binom{[n]}{k} := \{(x_1, \ldots, x_k) \mid x_i \in \{1, 2, \ldots, n\}, x_1 < \cdots < x_k\},$$

and for a matrix A we denote its i-th row by $A[i]$, its i-th column by A_i, and the entry in the i-th row and the j-th column by $A_{i,j}$.

2.1 Lifted Gabidulin (LG) Codes

For two $k \times \ell$ matrices A and B over $\mathbb{F}_q$ the *rank distance* is defined by

$$d_R(A, B) \overset{\text{def}}{=} \mathrm{rank}(A - B) \ .$$

A $[k \times \ell, \varrho, \delta]$ *rank-metric code* C is a linear subspace with dimension ϱ of $\mathbb{F}_q^{k \times \ell}$, in which each two distinct codewords A and B have distance $d_R(A, B) \geq \delta$. For a $[k \times \ell, \varrho, \delta]$ rank-metric code C it was proven in [2,5,18] that

$$\varrho \leq \min\{k(\ell - \delta + 1), \ell(k - \delta + 1)\} \ . \tag{2}$$

The codes which attain this bound are called *maximum rank distance* codes (or MRD codes in short).

An important family of MRD linear codes was presented by Gabidulin [5]. These codes can be seen as the analogs of Reed-Solomon codes for the rank metric. From now on let $k \leq \ell$. A codeword A in a $[k \times \ell, \varrho, \delta]$ rank-metric code C, can be represented by a vector $c_A = (c_1, c_2, \ldots, c_k)$, where $c_i = {\phi^{(\ell)}}^{-1}(A[i]) \in \mathbb{F}_{q^\ell}$. Let $g_i \in \mathbb{F}_{q^\ell}$, $h_i \in \mathbb{F}_{q^\ell}$, $1 \leq i \leq k$, be two sets of linearly independent over $\mathbb{F}_q$ elements. Then the generator matrix G and the parity-check matrix H of a $[k \times \ell, \varrho, \delta]$ Gabidulin MRD code are given by

$$G = \begin{pmatrix} g_1 & g_2 & \cdots & g_k \\ g_1^{[1]} & g_2^{[1]} & \cdots & g_k^{[1]} \\ g_1^{[2]} & g_2^{[2]} & \cdots & g_k^{[2]} \\ \vdots & \vdots & \vdots & \vdots \\ g_1^{[k-\delta]} & g_2^{[k-\delta]} & \cdots & g_k^{[k-\delta]} \end{pmatrix}, H = \begin{pmatrix} h_1 & h_2 & \cdots & h_k \\ h_1^{[1]} & h_2^{[1]} & \cdots & h_k^{[1]} \\ h_1^{[2]} & h_2^{[2]} & \cdots & h_k^{[2]} \\ \vdots & \vdots & \vdots & \vdots \\ h_1^{[\delta-2]} & h_2^{[\delta-2]} & \cdots & h_k^{[\delta-2]} \end{pmatrix},$$

where $\varrho = \ell(k - \delta + 1)$, and $[i] = q^i$ [5].

Let A be a $k \times \ell$ matrix over $\mathbb{F}_q$ and let I_k be the $k \times k$ identity matrix. The matrix $[I_k\ A]$ can be viewed as a generator matrix of a k-dimensional subspace of $\mathbb{F}_q^{k+\ell}$. This subspace is called the *lifting* of A [20].

When the codewords of a rank-metric code C are lifted to k-dimensional subspaces, the result is a constant dimension code $\mathcal{C}$. If C is a Gabidulin MRD code then $\mathcal{C}$ is called a *lifted Gabidulin (LG) code* [20].

Theorem 1 *[20] Let k, n be positive integers such that $k \leq n-k$. If C is a $[k \times (n-k), (n-k)(k-\delta+1), \delta]$ Gabidulin MRD code then $\mathcal{C}$ is an $(n, q^{(n-k)(k-\delta+1)}, 2\delta, k)_q$ constant dimension code.*

2.2 The Plücker Embedding

The basic idea of using the Plücker embedding for list decoding of subspace codes was already stated in [17,23]. We will now recall the main definitions and theorems from those works. The proofs of the results can also be found in there. For more information or a more general formulation of the Plücker embedding and its applications the interested reader is referred to [9].

Let $U \in \mathbb{F}_q^{k \times n}$ such that its row space $\mathrm{rs}(U)$ describes the subspace $\mathcal{U} \in \mathcal{G}_q(k,n)$. $M_{i_1,\ldots,i_k}(U)$ denotes the minor of U given by the columns $i_1, \ldots, i_k$. The Grassmannian $\mathcal{G}_q(k,n)$ can be embedded into projective space using the Plücker embedding:

$$\begin{aligned} \varphi : \mathcal{G}_q(k,n) &\longrightarrow \mathbb{P}^{\binom{n}{k}-1} \\ \mathrm{rs}(U) &\longmapsto [M_{1,\ldots,k}(U) : M_{1,\ldots,k-1,k+1}(U) : \ldots : M_{n-k+1,\ldots,n}(U)]. \end{aligned}$$

The $k \times k$ minors $M_{i_1,\ldots,i_k}(U)$ of the matrix U are called the *Plücker coordinates* of the subspace $\mathcal{U}$. By convention, we order the minors lexicographically by the column indices.

The image of this embedding describes indeed a variety and the defining equations of the image are given by the so called *shuffle relations* (see e.g. [10,16]), which are multilinear equations of monomial degree 2 in terms of the Plücker coordinates:

Proposition 2 *Consider $x := [x_{1,\ldots,k} : \cdots : x_{n-k+1,\ldots,n}] \in \mathbb{P}^{\binom{n}{k}-1}$. Then there exists a $\mathcal{U} \in \mathcal{G}_q(k,n)$ such that $\varphi(\mathcal{U}) = x$ if and only if*

$$\sum_{\sigma \in S_{2k}} \mathrm{sgn}(\sigma) x_{\sigma(i_1,\ldots,i_k)} x_{\sigma(i_{k+1},\ldots,i_{2k})} = 0 \quad \forall (i_1, \ldots, i_{2k}) \in \binom{[n]}{2k}.$$

Then one can easily count the number of different shuffle equations.

Lemma 3 *There are $\binom{n}{2k}$ shuffle relations defining $\mathcal{G}_q(k,n)$ in the Plücker embedding.*

Example 4 *$\mathcal{G}_q(2,4)$ is described by a single relation:*

$$x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23} = 0.$$

The balls of radius $2t$ (with respect to the subspace distance) around some $\mathcal{U} \in \mathcal{G}_q(k,n)$ can be described by explicit equations in the Plücker embedding. For it we need the *Bruhat order*:

$$(i_1,...,i_k) \geq (j_1,...,j_k) \iff i_l \geq j_l \quad \forall l \in \{1,\dots,k\}.$$

Note, that the Bruhat order is not a total but only a partial order on $\binom{[n]}{k}$.

Example 5 *According to the Bruhat order it holds that $(1,2,7) \leq (2,3,7)$. But the fact that $(2,4,6) \not\leq (2,3,7)$ does not imply that $(2,4,6) > (2,3,7)$. These two tuples are not comparable.*

The equations defining the balls are easily determined in the following special case:

Proposition 6 *[9,17] Define $\mathcal{U}_0 := \mathrm{rs}[\,I_k\ 0_{k\times n-k}\,]$. Then*

$$B_{2t}(\mathcal{U}_0) = \{\mathcal{V} = \mathrm{rs}(V) \in \mathcal{G}_q(k,n) \mid M_{i_1,\dots,i_k}(V) = 0 \\ \forall (i_1,...,i_k) \not\leq (t+1,\dots,k,n-t+1,...,n)\}.$$

With the knowledge of $B_{2t}(\mathcal{U}_0)$ we can also express $B_{2t}(\mathcal{U})$ for any $\mathcal{U} \in \mathcal{G}_q(k,n)$. For this note, that for any $\mathcal{U} \in \mathcal{G}_q(k,n)$ there exists an $A \in GL_n$ such that $\mathcal{U}_0 A = \mathcal{U}$. Moreover,

$$B_{2t}(\mathcal{U}_0 A) = B_{2t}(\mathcal{U}_0)A.$$

The following results are taken from [17], where also the respective proofs can be found.

For simplifying the computations we define $\bar{\varphi}$ on GL_n, where we denote by $A[i_1,\dots,i_k]$ the submatrix of A that consists of the rows $i_1,\dots,i_k$:

$$\bar{\varphi} : GL_n \longrightarrow GL_{\binom{n}{k}}$$
$$A \longmapsto \begin{pmatrix} \det A_{1,\dots,k}[1,\dots,k] & \dots & \det A_{n-k+1,\dots,n}[1,\dots,k] \\ \vdots & & \vdots \\ \det A_{1,\dots,k}[n-k+1,\dots,n] & \dots & \det A_{n-k+1,\dots,n}[n-k+1,\dots,n] \end{pmatrix}$$

Lemma 7 *Let $\mathcal{U} \in \mathcal{G}_q(k,n)$ and $A \in GL_n$. It holds that*

$$\varphi(\mathcal{U}A) = \varphi(\mathcal{U})\bar{\varphi}(A).$$

Theorem 8 *Let $\mathcal{U} = \mathcal{U}_0 A \in \mathcal{G}_q(k,n)$. Then*

$$B_{2t}(\mathcal{U}) = B_{2t}(\mathcal{U}_0 A) = \{\mathcal{V} \in \mathcal{G}_q(k,n) \mid M_{i_1,\dots,i_k}(V)\bar{\varphi}(A^{-1}) = 0 \\ \forall (i_1,\dots,i_k) \not\leq (t+1,\dots,k,n-t+1,...,n)\}.$$

There are always several choices for $A \in GL_n$ such that $\mathcal{U}_0 A = \mathcal{U}$. Since $GL_{\binom{n}{k}}$ is very large we try to choose A as simple as possible. We will now explain one such construction.

Construction 1 *For a given $\mathcal{U} = \mathrm{rs}(U) \in \mathcal{G}_q(k,n)$ we construct $A \in GL_n$ such that $\mathcal{U}_0 A = \mathcal{U}$ as follows:*

1. *The first k rows of A are equal to the matrix representation U of $\mathcal{U}$.*
2. *Find the pivot columns of U (assume that U is in RREF).*
3. *Fill up the respective columns of A with zeros in the lower $n-k$ rows.*
4. *Fill up the remaining submatrix of size $n-k \times n-k$ with an identity matrix.*

Then the inverse of A can be computed as follows:

1. *Find a permutation $\sigma \in S_n$ that permutes the columns of A such that*

$$\sigma(A) = \begin{pmatrix} I_k & U'' \\ 0 & I_{n-k} \end{pmatrix}.$$

2. *Then the inverse of that matrix is*

$$\sigma(A)^{-1} = \begin{pmatrix} I_k & -U'' \\ 0 & I_{n-k} \end{pmatrix}.$$

3. *Apply σ on the rows of $\sigma(A)^{-1}$. The result is A^{-1}. One can easily see this if one represents σ by a matrix S. Then one gets $(SA)^{-1}S = A^{-1}S^{-1}S = A^{-1}$.*

Thus, we know how to describe the balls of a given radius $2t$ around an element of $\mathcal{G}_q(k,n)$ with linear equations in the Plücker embedding, which is exactly what is needed for a list decoding algorithm. In the following section we will describe a way of representing a subset of the Plücker coordinates of lifted rank-metric codes as linear block codes, which can then be used to come up with a list decoding algorithm in the Plücker embedding.

3 List Decoding LG Codes in the Plücker Embedding

3.1 Linear Block Codes over $\mathbb{F}_q$ in the Plücker Coordinates of LG Codes

Let C be an $[k \times (n-k), (n-k)(k-\delta+1, \delta)]$ Gabidulin MRD code over $\mathbb{F}_q$. Then by Theorem 1 its lifting is a code $\mathcal{C}$ of size $q^{(n-k)(k-\delta+1)}$ in the Grassmannian $\mathcal{G}_q(k,n)$. Let

$$x^{\mathcal{A}} = [x^{\mathcal{A}}_{1\dots k} : \dots : x^{\mathcal{A}}_{n-k+1\dots n}] \in \mathbb{P}^{\binom{n}{k}-1}$$

be a vector which represents the Plücker coordinates of a subspace $\mathcal{A} \in \mathcal{G}_q(k,n)$. If $x^{\mathcal{A}}$ is normalized (i.e. the first non-zero entry is equal to one), then $x^{\mathcal{A}}_{1\dots k} = 1$ for any $\mathcal{A} \in \mathcal{C}$.

Let $[k] = \{1,2,\dots,k\}$, and let $\underline{i} = \{i_1, i_2, \dots, i_k\}$ be a set of indices such that $|\underline{i} \cap [k]| = k-1$. Let $t \in \underline{i}$, such that $t > k$, and $s = [k] \setminus \underline{i}$.

Lemma 9 *Consider $A \in C$ and $\mathcal{A} = \mathrm{rs}[\ I_k\ A\ ]$. If $x^{\mathcal{A}}$ is normalized, then $x^{\mathcal{A}}_{\underline{i}} = (-1)^{k-s} A_{s,t-k}$.*

Proof It holds that $x^{\mathcal{A}}$ is normalized if its entries are the minors of the reduced row echelon form of $\mathcal{A}$, which is $[\ I_k\ A\ ]$. Because of the identity matrix in the first k columns, the statement follows directly from the definition of the Plücker coordinates. □

Note, that we have to worry about the normalization since $x^{\mathcal{A}}$ is projective. In the following we will always assume that any element from $\mathbb{P}^{\binom{n}{k}-1}$ is normalized.

With Lemma 9 one can easily show, that a subset of the Plücker coordinates of a lifted Gabidulin code form a linear code over $\mathbb{F}_q$:

Theorem 10 *The restriction of the set of Plücker coordinates of an $(n, q^{(n-k)(k-\delta+1)}, 2\delta, k)_q$ lifted Gabidulin code $\mathcal{C}$ to the set $\{\underline{i} : |\underline{i}| = k, |\underline{i} \cap [k]| = k-1\}$ forms a linear code C^p over $\mathbb{F}_q$ of length $k(n-k)$, dimension $(n-k)(k-\delta+1)$ and minimum distance $d_{min} \geq \delta$.*

Proof Since C is linear, it holds that for every $A, B \in C$ we have $A + B \in C$. Together with Lemma 9 we have the same property when we consider the restriction of the set of Plücker coordinates of a lifted Gabidulin code to the set $\{\underline{i} : |\underline{i}| = k, |\underline{i} \cap [k]| = k-1\}$. This set is of size $k(n-k)$, and therefore we obtain a linear code C^p of length $k(n-k)$ and the same dimension as C, i.e. $(n-k)(k-\delta+1)$. Since the rank of each non-zero $A \in C$ is greater or equal to δ, also the number of non-zero entries of A has to be greater or equal to δ, hence the minimum Hamming distance d_{min} of C^p satisfies $d_{min} \geq \delta$. □

Example 11 *Let $\alpha \in \mathbb{F}_{2^2}$ be a primitive element, fulfilling $\alpha^2 = \alpha + 1$. Let C be a $[2 \times 2, 2, \delta = 2]$ Gabidulin MRD code over $\mathbb{F}_2$ with parity-check and generator matrices given by*

$$H = (1\ \alpha) \text{ and } G = (\alpha\ 1),$$

respectively. Hence, we want to lift $C = \{(b\alpha, b) : b \in \mathbb{F}_{2^2}\}$. The codewords of C, their representation as 2×2 matrices, their lifting to $\mathcal{G}_2(2,4)$ and the respective Plücker coordinates are given in the following table.

vector representation	*matrix representation*	*lifting*	*Plücker coordinates*
$(0,0)$	$\begin{pmatrix} 0\,0 \\ 0\,0 \end{pmatrix}$	$\begin{pmatrix} 1\,0\,0\,0 \\ 0\,1\,0\,0 \end{pmatrix}$	$[1:0:0:0:0:0]$
$(\alpha,1)$	$\begin{pmatrix} 0\,1 \\ 1\,0 \end{pmatrix}$	$\begin{pmatrix} 1\,0\,0\,1 \\ 0\,1\,1\,0 \end{pmatrix}$	$[1:1:0:0:1:1]$
(α^2,α)	$\begin{pmatrix} 1\,1 \\ 0\,1 \end{pmatrix}$	$\begin{pmatrix} 1\,0\,1\,1 \\ 0\,1\,0\,1 \end{pmatrix}$	$[1:0:1:1:1:1]$
$(1,\alpha^2)$	$\begin{pmatrix} 1\,0 \\ 1\,1 \end{pmatrix}$	$\begin{pmatrix} 1\,0\,1\,0 \\ 0\,1\,1\,1 \end{pmatrix}$	$[1:1:1:1:0:1]$

In this example, $C^p = \{(0000), (1001), (0111), (1110)\}$. This is a $[4,2,2]$ linear code in the Hamming space. Its parity-check matrix is

$$H^p = \begin{pmatrix} 1\,0\,1\,1 \\ 0\,1\,1\,0 \end{pmatrix}.$$

In other words, a Plücker coordinate vector $[x_{12} : x_{13} : x_{14} : x_{23} : x_{24} : x_{34}]$ of a vector space from $\mathcal{G}_2(2,4)$ represents a codeword of the lifted Gabidulin code from above if and only if $x_{12} = 1$, $x_{14} + x_{23} = 0$, and $x_{13} + x_{23} + x_{24} = 0$.

3.2 The List Decoding Algorithm

We now have all the machinery needed to describe a list decoding algorithm for lifted rank-metric codes in the Plücker coordinates under the assumption that the received word has the same dimension as the codewords. Consider a lifted rank-metric code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ and denote its corresponding $[k(n-k), (n-k)(k-\delta+1)]$-linear block code over $\mathbb{F}_q$ by C^p. The corresponding parity check matrix is denoted by H^p. Let $\mathcal{R} = \mathrm{rs}(R) \in \mathcal{G}_q(k,n)$ be the received word. Let e be the number of errors (i.e. insertions and deletions) to be corrected.

We showed in Section 3.1 how a subset of the Plücker coordinates of a LG code forms a linear block code that is defined through the parity check matrix H^p. Since we want to describe a list decoding algorithm inside the whole set of Plücker coordinates, we define an extension of H^p as follows:

$$\bar{H}^p = \left(0_{(\delta-1)(n-k)\times 1}\ H^p\ 0_{(\delta-1)(n-k)\times \ell} \right)$$

where $\ell = \binom{n}{k} - k(n-k) - 1$. Then $[x_{1\dots k} : \dots : x_{n-k+1\dots n}]\bar{H}^{p^T} = 0$ gives rise to the same equations as $[x_{i_1} : \dots : x_{i_{k(n-k)}}]H^{p^T} = 0$, for $i_1, \dots, i_{k(n-k)} \in \underline{i}$. For simplicity we will sometimes write $\bar{x}$ for $[x_{1\dots k} : \dots : x_{n-k+1\dots n}]$ in the following.

Theorem 12 *Algorithm 1 outputs the complete list L of codewords (in Plücker coordinate representation), such that for each element $\bar{x} \in L$, $d_S(\varphi^{-1}(\bar{x}), \mathcal{R}) \le 2e$.*

Proof The solution set to the shuffle relations is exactly $\varphi(\mathcal{G}_q(k,n))$, i.e. all the elements of $\mathbb{P}^{\binom{n}{k}-1}$ that are Plücker coordinates of a k-dimensional vector space in $\mathbb{F}_q^n$. The subset of this set with the condition $x_{1,\dots,k} = 1$ is exactly the set of Plücker coordinates of elements in $\mathcal{G}_q(k,n)$ whose reduced row echelon form has I_k as the left-most columns. Intersecting this with the solution set of the equations given by H^p achieves the Plücker coordinates of the lifted code $\mathcal{C}$. The intersection with $B_{2e}(\mathcal{R})$ is then given by the additional equations from 1. in the algorithm. Thus the solution set to the whole system of equation is the Plücker equations of $\mathcal{C} \cap B_{2e}(\mathcal{R})$. □

Algorithm 1

Input: $\mathcal{R}$, e

1. Find the equations defining $B_{2e}(\mathcal{R})$ in the Plücker coordinates, like explained in Section 2.2.
2. Solve the system of equations, that arise from $\bar{x}\bar{H}^p = 0$, together with the equation of $B_{2e}(\mathcal{R})$, the shuffle relations and the equation $x_{1,\dots,k} = 1$.

Output: The solutions $\bar{x} = [x_{1\dots k} : \dots : x_{n-k+1\dots n}]$ of this system of equations.

For the analysis of complexity of this algorithm we need to calculate the number of equations, denoted by τ, that define a ball of radius $2e$.

Lemma 13 *The number of equations defining $B_{2e}(\mathcal{U}_0)$ is equal to the number of equations defining $B_{2e}(\mathcal{U})$ for any $\mathcal{U} \in \mathcal{G}_q(k,n)$.*

Proof Follows directly from Lemma 7. □

Since we can count the elements that are not less than or equal to a given element in the Bruhat order, we get:

Lemma 14 *The number of equations defining $B_{2e}(\mathcal{U})$ inside $\mathcal{G}_q(k,n)$ is*

$$\tau = \sum_{l=0}^{k-e-1} \binom{n-k}{k-l}\binom{k}{l} = \binom{n}{k} - \sum_{l=k-e}^{k} \binom{n-k}{k-l}\binom{k}{l}.$$

Proof The condition that $(i_1,\dots,i_k) \not\leq (e+1,\dots,k,n-t+1,\dots,n)$ is equivalent to

$$\exists l \in \{1,\dots,k-e\} : i_l > k.$$

For such an l there are $k-l+1$ entries chosen freely from $\{k+1,\dots,n\}$ and $l-1$ entries from $\{1,\dots,k\}$. Hence there are

$$\sum_{l=1}^{k-e} \binom{n-k}{k-l+1}\binom{k}{l-1} = \sum_{l=0}^{k-e-1} \binom{n-k}{k-l}\binom{k}{l}$$

many elements in $\binom{[n]}{k}$ that are $\not\leq (e+1,\dots,k,n-t+1,\dots,n)$, which is equal to the number of equations defining $B_{2e}(\mathcal{U})$. □

The complexity of Algorithm 1 is dominated by solving the system of $\tau+1+(\delta-1)(n-k)+\binom{n}{2k}$ linear and bilinear equations in $\binom{n}{k}$ variables. This has a complexity that is polynomial in n and exponential in k.

In most of the examples we computed though, we only needed a subset of all equations to get the solutions. For this note, that the actual information is encoded in the rank-metric code part of the matrix representation of the vector space, i.e. in the Plücker coordinates corresponding to C^p. Hence, one does not need the $k\times n$-matrix representation of the solutions from an application point of view, since the information can be extracted directly from the Plücker coordinate representation of the vector spaces. On the other hand, because of this structure it is also straight-forward to construct the matrix representation by using Lemma 9 (i.e. without any computation needed). So, the number of variables in the system could be reduced to $k(n-k)$, and this can decrease the complexity of the algorithm.

Example 15 *We consider the code from Example 11.*

1. *Assume we received*
$$\mathcal{R}_1 = \begin{pmatrix} 1\,0\,1\,0 \\ 0\,0\,0\,1 \end{pmatrix}.$$
We would like to correct one error. Thus we first find the equations for the ball of subspace radius 2:
$$B_2(\mathcal{U}_0) = \{\mathcal{V} = \mathrm{rs}(V) \in \mathcal{G}_2(2,4) \mid M_{3,4}(V) = 0\}$$
We construct A_1^{-1} according to Construction 1
$$A_1^{-1} = \begin{pmatrix} 1\,0\,0\,1 \\ 0\,0\,1\,0 \\ 0\,0\,0\,1 \\ 0\,1\,0\,0 \end{pmatrix}$$
and compute the last column of $\bar{\varphi}(A_1^{-1})$:
$$[1:0:0:1:0:0]^T.$$
Thus, we get that
$$B_2(\mathcal{R}_1) = \{\mathcal{V} = \mathrm{rs}(V) \in \mathcal{G}_2(2,4) \mid M_{1,4}(V) + M_{2,3}(V) = 0\}.$$
Then combining with the parity check equations from Example 11 we obtain the following system of linear equations to solve
$$\begin{aligned} x_{13} + x_{14} + x_{24} &= 0 \\ x_{14} + x_{23} &= 0 \\ x_{12} + x_{23} &= 0 \\ x_{12} &= 1 \end{aligned}$$
where the first two equations arise from $\bar{H}^p$, the third from $B_2(\mathcal{R}_1)$ and the last one is the always given one. This system has the two solutions $(1,1,1,1,0)$ and $(1,0,1,1,1)$ for $(x_{12}, x_{13}, x_{14}, x_{23}, x_{24})$. Since we used all the equations defining the ball in the system of equations, we know that the two codewords corresponding to these two solutions (i.e. the third and fourth in Example 11) are the ones with distance 2 from the received space, and we do not have to solve x_{34} at all. The corresponding codewords are
$$\begin{pmatrix} 1\,0\,1\,0 \\ 0\,1\,1\,1 \end{pmatrix}, \begin{pmatrix} 1\,0\,1\,1 \\ 0\,1\,0\,1 \end{pmatrix}.$$
2. *Now assume we received*
$$\mathcal{R}_2 = \begin{pmatrix} 1\,0\,0\,1 \\ 0\,1\,1\,1 \end{pmatrix}.$$
As previously, we construct A_2^{-1} according to Construction 1
$$A_2^{-1} = \begin{pmatrix} 1\,0\,0\,1 \\ 0\,1\,1\,1 \\ 0\,0\,1\,0 \\ 0\,0\,0\,1 \end{pmatrix}$$
and compute the last column of $\bar{\varphi}(A_2^{-1})$:
$$[1:1:0:1:1:1]^T.$$
Thus, we get that
$$B_2(\mathcal{R}_1) = \{\mathcal{V} = \mathrm{rs}(V) \in \mathcal{G}_2(2,4) \mid M_{1,2}(V) + M_{1,3}(V) + M_{2,3}(V) + M_{2,4}(V) + M_{3,4}(V) = 0\}.$$

Then combining with the parity check equations from Example 11 and the shuffle relation from Example 4 we obtain the following system of linear and bilinear equations

$$\begin{aligned} x_{13}+x_{14}+x_{24} &= 0 \\ x_{14}+x_{23} &= 0 \\ x_{12}+x_{13}+x_{23}+x_{24}+x_{34} &= 0 \\ x_{12}x_{34}+x_{13}x_{24}+x_{14}x_{23} &= 0 \\ x_{12} &= 1 \end{aligned}$$

We rewrite these equations in terms of variables $x_{13}, x_{14}, x_{23}, x_{24}$ which correspond to a lifted Gabidulin code as follows.

$$\begin{aligned} x_{13}+x_{14}+x_{24} &= 0 \\ x_{14}+x_{23} &= 0 \\ x_{1,3}+x_{2,3}+x_{2,4}+x_{13}x_{24}+x_{14}x_{23} &= 1 \end{aligned}$$

This system has three solutions $(1,0,0,1)$, $(0,1,1,1)$, and $(1,1,1,0)$ for $(x_{13}, x_{14}, x_{23}, x_{24})$. The corresponding codewords are

$$\begin{pmatrix} 1\,0\,0\,1 \\ 0\,1\,1\,0 \end{pmatrix}, \begin{pmatrix} 1\,0\,1\,1 \\ 0\,1\,0\,1 \end{pmatrix}, \begin{pmatrix} 1\,0\,1\,0 \\ 0\,1\,1\,1 \end{pmatrix}.$$

Remark 16 *Note that an upper and a lower bounds for the list size, i.e. the number of codewords in a ball of subspace radius $2e$ around a received word, can be directly derived from the bounds on a list size of a classical Gabidulin code, given rank radius e. This result follows from the next lemma.*

Lemma 17 *Let $\mathcal{R} \in \mathcal{G}_q(k,n)$ and denote by $R \in \mathbb{F}_q^{k\times n}$ its reduced row echelon form. Then for any $A \in \mathbb{F}_q^{k\times(n-k)}$ there always exists a matrix $M \in \mathbb{F}_q^{k\times(n-k)}$ such that $d_S(\mathcal{R}, \mathrm{rs}[\ I_k\ \ A\ ]) = d_S(\mathrm{rs}[\ I_k\ M\ ], \mathrm{rs}[\ I_k\ A\ ])$.*

Proof Because of the reduced row echelon form it holds that there exists $\bar{M} \in \mathbb{F}_q^{k\times n-k}$ such that

$$\mathrm{rank}\begin{pmatrix} I_k & A \\ & R \end{pmatrix} = \mathrm{rank}\begin{pmatrix} I_k & A \\ 0_{k\times k} & \bar{M} \end{pmatrix}$$

which implies that $d_S(\mathcal{R}, \mathrm{rs}[\ I_k\ \ A\ ]) = d_S(\mathrm{rs}[\ I_k\ \ A+\bar{M}\ ], \mathrm{rs}[\ I_k\ \ A\ ])$. With $M := A+\bar{M}$, the statement follows. □

Bounds for the list size for classical Gabidulin list decoding can be found e.g. in [26].

4 Conclusion and Open Problems

We presented a list decoding algorithm for lifted Gabidulin codes that works by solving a system of linear and bilinear equations in the Plücker coordinates. In contrast to the algorithms presented in [8, 14] this algorithm works for lifted Gabidulin codes for any set of parameters q, n, k, δ.

One can easily extend the algorithm presented in this paper to work also for received spaces of a different dimension. For this, one only needs to change the conditions in Proposition 6 indicating which Plücker coordinates have to be zero. The rest of the theory can then be carried over straightforwardly. In a similar manner one can make the algorithm work for unions of LG codes of different length (cf. e.g. [21]). To do so, one needs to add a preliminary step in the algorithm where a rank argument decides, which of these LG codes can possibly have codewords that are in the ball around the received word.

The storage needed for our algorithm is fairly little, the complexity is polynomial in n but exponential in k. Since in applications, k is quite small while n tends to get large, this is still reasonable. In future work, we still want to improve this complexity by trying to decrease the size of the system of equations to solve in the last step of the algorithm. Moreover, it would be interesting to see if some converse version of Theorem 10 exists, i.e. if one can generate constant dimension codes from a given linear block code by using this as a subset of the Plücker coordinates of the constant dimension code. Moreover, we would like to find other families of codes that can be described through equations in their Plücker coordinates and use this fact to come up with list decoding algorithms of these other codes.

References

1. M. Bossert and E. M. Gabidulin, *One family of algebraic codes for network coding*, In Proceedings of the IEEE International Symposium on Information Theory, pages 2863 - 2866, 2009.
2. P. Delsarte, *Bilinear forms over a finite field, with applications to coding theory*, J. Combin. Theory Ser. A **25** (1978), no. 3, 226–241.
3. T. Etzion and N. Silberstein, "Error-correcting codes in projective space via rank-metric codes and Ferrers diagrams", *IEEE Trans. Inform. Theory*, vol. 55, no.7, pp. 2909–2919, July 2009.
4. T. Etzion and A. Vardy, "Error-correcting codes in projective space", *IEEE Trans. Inform. Theory*, vol. 57, no. 2, pp. 1165–1173, February 2011.
5. È. M. Gabidulin, *Theory of codes with maximum rank distance*, Problemy Peredachi Informatsii **21** (1985), no. 1, 3–16.
6. M. Gadouleau and Z. Yan, "Constant-rank codes and their connection to constant-dimension codes," *IEEE Trans. Inform. Theory*, vol. 56, no. 7, pp. 3207–3216, July 2010.
7. V. Guruswami, S. Narayanan, and C. Wang. *List decoding subspace codes from insertions and deletions*, In Proceedings of Innovations in Theoretical Computer Science (ITCS 2012), pages 183189, January 2012.
8. V. Guruswami and C. Xing, *List decoding Reed-Solomon, Algebraic-Geometric, and Gabidulin subcodes up to the Singleton bound*, electronic collloquium on computationl complexity, report No. 146 (2012).
9. W. V. D. Hodge and D. Pedoe, *Methods of algebraic geometry, vol. ii*, vol. 2, Cambridge University Press, 1952.
10. S. L. Kleiman and D. Laksov, *Schubert calculus*, Amer. Math. Monthly **79** (1972), 1061–1082.
11. A. Kohnert and S. Kurz, "Construction of large constant-dimension codes with a prescribed minimum distance," *Lecture Notes in Computer Science*, vol. 5393, pp. 31–42, December 2008.
12. R. Kötter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Inform. Theory*, vol. 54, no. 8, pp. 3579–3591, August 2008.
13. F. Manganiello, E. Gorla, and J. Rosenthal, "Spread codes and spread decoding in network coding", in proceedings of *International Symposium on Information Theory*, pp. 881–885, Toronto, Ontario, Canada, July 2008.
14. H. Mahdavifar and A. Vardy. *List-decoding of subspace codes and rank-metric codes up to Singleton bound*, CoRR, abs/1202.0866, 2012
15. H. Mahdavifar and A. Vardy. *Algebraic list-decoding on the operator channel*, In Proceedings of the IEEE International Symposium on Information Theory, pages 11931197, 2010.
16. C. Procesi, *A primer of invariant theory*, Brandeis lecture notes, Brandeis University, 1982, Notes by G. Boffi.
17. J. Rosenthal and A.-L. Trautmann, *Decoding of subspace codes, a problem of schubert calculus over finite fields*, arXiv:1209.2887 [**cs.IT**] (2012).
18. R.M. Roth, *Maximum-rank array codes and their application to crisscross error correction*, Information Theory, IEEE Transactions on **37** (1991), no. 2, 328 –336.
19. N. Silberstein and T. Etzion, "Codes and Designs Related to Lifted MRD Codes", in proceedings of *International Symposium on Information Theory*, pp. 2199–2203, Saint Petersburg, Russia, August 2011.
20. D. Silva, F.R. Kschischang, and R. Kötter, *A rank-metric approach to error control in random network coding*, Information Theory, IEEE Transactions on **54** (2008), no. 9, 3951 –3967.
21. V. Skachek, "Recursive code construction for random networks," *IEEE Trans. Inform. Theory*, vol. 56, no. 3, pp. 1378–1382, March 2010.
22. A.-L. Trautmann, F. Manganiello, M. Braun, and J. Rosenthal, *Cyclic orbit codes*, CoRR, 01112.1238v1, 2011.
23. A.-L. Trautmann, *Plücker embedding of cyclic orbit codes*, Proceedings of the 20th International Symposium on Mathematical Theory of Networks and Systems – MTNS (Melbourne, Australia), 2012, pp. 1–15.
24. A.-L. Trautmann, F. Manganiello, and J. Rosenthal, "Orbit codes- a new concept in the area of network coding", in proc. of *Inf. Theory Workshop (ITW)*, pp. 1–4, 2010 IEEE, Dublin, Ireland, August 2010.
25. A.-L. Trautmann and J. Rosenthal, "New improvements on the echelon-Ferrers construction", in proc. of *Int. Symp. on Math. Theory of Networks and Systems*, pp. 405–408, July 2010.
26. A. Wachter-Zeh. *Bounds on list decoding Gabidulin codes*, CoRR, abs/1205.0345, 2012