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

On the Geometry of Balls in the Grassmannian and List Decoding of Lifted Gabidulin Codes

Joachim Rosenthal · Natalia Silberstein · Anna-Lena Trautmann

the date of receipt and acceptance should be inserted later

Abstract The finite Grassmannian $\mathcal{G}_q(k,n)$ is defined as the set of all k-dimensional subspaces of the ambient space $\mathbb{F}_q^n$. Subsets of the finite Grassmannian are called constant dimension codes and have recently found an application in random network coding. In this setting codewords from $\mathcal{G}_q(k,n)$ are sent through a network channel and, since errors may occur during transmission, the received words can possibly lie in $\mathcal{G}_q(k',n)$, where $k' \neq k$.

In this paper, we study the balls in $\mathcal{G}_q(k,n)$ with center that is not necessarily in $\mathcal{G}_q(k,n)$. We describe the balls with respect to two different metrics, namely the subspace and the injection metric. Moreover, we use two different techniques for describing these balls, one is the Plücker embedding of $\mathcal{G}_q(k,n)$, and the second one is a rational parametrization of the matrix representation of the codewords.

With these results, we consider the problem of list decoding a certain family of constant dimension codes, called lifted Gabidulin codes. We describe a way of representing these codes by linear equations in either the matrix representation or a subset of the Plücker coordinates. The union of these equations and the linear and bilinear equations which arise from the description of the ball of a given radius provides an explicit description of the list of codewords with distance less than or equal to the given radius from the received word.

Keywords Grassmannian · projective space · subspace codes · network coding · list decoding

Mathematics Subject Classification (2010) 11T71,14G50

1 Introduction

Let $\mathbb{F}_q$ be a finite field of size q and let k, n be two integers satisfying $0 \leq k \leq n$. The *Grassmannian space* (Grassmannian, in short), denoted by $\mathcal{G}_q(k,n)$, is the set of all k-dimensional subspaces of

J. Rosenthal and A.-L. Trautmann were partially supported by Swiss National Science Foundation Grant no. 138080. A.-L. Trautmann was partially supported by Forschungskredit of the University of Zurich, grant no. 57104103, and Swiss National Science Foundation Fellowship no. 147304.

Parts of this work were presented at the International Workshop on Coding and Cryptography 2013 in Bergen, Norway, and appear in its proceedings [30].

J. Rosenthal
Institute of Mathematics, University of Zurich, Switzerland
E-mail: rosenthal@math.uzh.ch

A.-L. Trautmann
Department of Electrical and Electronic Engineering, University of Melbourne, Australia
E-mail: anna-lena.trautmann@unimelb.edu.au

N. Silberstein
Department of Computer Science, Technion — Israel Institute of Technology, Haifa, Israel
E-mail: natalys@cs.technion.ac.il

the vector space $\mathbb{F}_q^n$. Let $\mathcal{U}, \mathcal{V} \subset \mathbb{F}_q^n$ be two different subspaces in $\mathcal{G}_q(k,n)$. The *subspace distance* is defined by

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

A subset $\mathcal{C}$ of $\mathcal{G}_q(k,n)$ is called an $(n, M, d, k)_q$ *constant dimension code* if it has size M and if the minimum pairwise subspace distance between any two different subspaces of $\mathcal{C}$ is d.

Constant dimension codes gained a lot of interest due to the work by Kötter and Kschischang [16] who showed that such codes are very useful for error-correction in random network coding. They proved that an $(n, M, d, k)_q$ code can correct any μ packet insertions (which is equivalent to an increase of dimension by μ in the transmitted subspace) and ϵ packet deletions (which is equivalent to a decrease of dimension by ϵ) introduced anywhere in the network as long as $2\mu + 2\epsilon < d$. This application has motivated extensive work in the area [1,4,6,8,9,11,15,17, 19,18,21,23,24,26,32,33]. In [16] Kötter and Kschischang gave a Singleton-like upper bound on the size of such codes and presented a Reed-Solomon-like code which asymptotically attains this bound. Silva, Kötter, and Kschischang [25] showed how this construction can be described in terms of lifted Gabidulin codes [7]. The generalizations of this construction and the decoding algorithms were presented in [1,4,17,21,26,33]. Another type of construction (orbit codes) can be found in [6, 15,32].

In this paper we focus on describing the balls of a given radius in the Grassmannian around an arbitrary element of the respective projective space. This is exactly what is needed to come up with list decoding algorithms for constant dimension codes. Then we focus on list decoding of lifted Gabidulin codes. For the classical Gabidulin codes it was recently shown by Wachter-Zeh [34] that, if the radius of the ball around a received word is at least 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 [9,19]. The constructions of subcodes of (lifted) Gabidulin codes and their algebraic list decoding algorithms were presented in [10,11,18,35].

One approach in this paper for list decoding codes in the Grassmannian is to apply the techniques of Schubert calculus over finite fields, i.e. to represent subspaces in the Grassmannian by their Plücker coordinates. It was proven in [21] 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 extend this result to the injection distance, which is interesting for the case when a ball around a subspace of a different dimension $k' \neq k$ is considered. Also, 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 linear equations combined with the bilinear equations defining the Grassmannian in the Plücker embedding will constitute the resulting list of codewords. Another approach considered in this paper is the description of the balls (for both the subspace and the injection distance) around a subspace by bilinear equations from a rational parametrization of the matrix representation of elements of $\mathcal{G}_q(k,n)$.

The paper is organized as follows. In Section 2 we review the Plücker embedding of the Grassmannian $\mathcal{G}_q(k,n)$. In Section 3 we describe the balls of radius t around some subspace of $\mathbb{F}_q^n$. We give the defining equations in Plücker coordinates and also describe a rational parametrization which will make the algorithmic computation for many list decoding problems easier. Section 4 contains the description of the lifted Gabidulin codes as linear block codes. Finally Section 5 contains two list decoding algorithms where we show how the set of equations describing a ball of some radius and the equations describing the lifting of the Gabidulin code can be computed. Conclusions and problems for future research are given in Section 6.

2 Preliminaries and Notations

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

We represent some $\mathcal{U} \in \mathcal{G}_q(k,n)$ by the row space of a matrix $U \in \mathbb{F}_q^{k\times n}$, where we use the notation $\mathrm{rs}(U)$ for the row space of U. GL_n acts on $\mathcal{G}_q(k,n)$ as follows:

$$\begin{aligned}\mathcal{G}_q(k,n) \times GL_n &\to \mathcal{G}_q(k,n)\\ (\mathrm{rs}(U), A) &\mapsto \mathrm{rs}(UA).\end{aligned}$$

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: The set of ordered multiindices of length k with elements from $\{1,2,\ldots,n\}$ is denoted by

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

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 $A_{i,j}$.

Example 1

$$\binom{[4]}{2} = \{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}$$

Definition 1 The *Bruhat order* on the set $\binom{[n]}{k}$, is defined as

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

The *lexicographic order* is defined as,

$$(i_1,\ldots,i_k) < (j_1,\ldots,j_k) \iff \exists 0 \le N \le k : i_m = j_m \forall m \le N \text{ and } i_{N+1} < j_{N+1}.$$

One notes that the Bruhat order is a partial order and the lexicographic order is a total order on $\binom{[n]}{k}$.

Example 2 According to the Bruhat order it holds that $(1,2,7) \preceq (2,3,7)$. But the fact that $(2,4,6) \not\preceq (2,3,7)$ does not imply that $(2,3,7) \prec (2,4,6)$. These two tuples are not comparable. In the lexicographic order it holds that $(1,2,7) < (2,3,7)$ and $(2,3,7) < (2,4,6)$.

We denote by $\mathcal{P}_q(n)$ the set of all subspaces of $\mathbb{F}_q^n$, i.e.,

$$\mathcal{P}_q(n) := \bigcup_{0\le k\le n} \mathcal{G}_q(k,n).$$

Definition 2 Let $\mathcal{U},\mathcal{V} \in \mathcal{P}_q(n)$ be two subspaces. The *subspace distance* is defined as

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

and the *injection distance* is definded as

$$d_I(\mathcal{U},\mathcal{V}) = \max(\dim(\mathcal{U}),\dim(\mathcal{V})) - \dim(\mathcal{U}\cap\mathcal{V}).$$

Clearly both distance functions describe a metric in the usual way. One also notes that for $\mathcal{U},\mathcal{V} \in \mathcal{G}_q(k,n)$ it holds that $d_S(\mathcal{U},\mathcal{V}) = 2d_I(\mathcal{U},\mathcal{V})$. Moreover, for constant dimension codes a unique subspace distance decoder is equivalent to a unique injection distance decoder [31]. For list decoding we will derive a similar relation between the two metrics in Proposition 14.

Definition 3 We define the balls in $\mathcal{G}_q(k,n)$ with subspace radius τ around an arbitrary element $\mathcal{R} \in \mathcal{P}_q(n)$ as

$$B^k_{S,\tau}(\mathcal{R}) := \{\mathcal{V} \in \mathcal{G}_q(k,n) \mid d_S(\mathcal{R},\mathcal{U}) \leq \tau\}.$$

Analogously we define the balls in $\mathcal{G}_q(k,n)$ with injection radius t around an arbitrary element $\mathcal{R} \in \mathcal{P}_q(n)$ as

$$B^k_{I,t}(\mathcal{R}) := \{\mathcal{V} \in \mathcal{G}_q(k,n) \mid d_I(\mathcal{R},\mathcal{U}) \leq t\}.$$

The Plücker embedding of the Grassmannian is a useful tool when studying $\mathcal{G}_q(k,n)$. The basic idea of using the Plücker embedding for list decoding of subspace codes was already stated in [21, 29]. 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 [12].

Remark 4 The condition $d_S(\mathcal{R},\mathcal{U}) \leq \tau$ (respectively $d_I(\mathcal{R},\mathcal{U}) \leq t$) translates into the condition that a subspace $\mathcal{U}$ should intersect the received space $\mathcal{R}$ in at least a certain dimension. Geometrically this describes a so called "Schubert condition" and actually both $B^k_{S,\tau}(\mathcal{R})$ and $B^k_{I,t}(\mathcal{R})$ have the structure of a so called "Schubert variety". Readers familiar with Schubert calculus as described in [12] will readily recognize this and it will not come as a surprise that the Plücker equations which describe the balls will turn out to be linear. In order to keep the paper as self contained as possible we will derive in this paper the relevant equations.

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 (i.e. the determinant of the submatrix) of U given by the columns $i_1,\ldots,i_k$. The Grassmannian $\mathcal{G}_q(k,n)$ can be embedded into the projective space $\mathbb{P}^{\binom{n}{k}-1}$ of dimension $\binom{n}{k}-1$ over $\mathbb{F}_q$ 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. [14,20]), which are multilinear equations of monomial degree 2 in terms of the Plücker coordinates:

Proposition 5 ([14,20]) *Consider $x := [x_{1,\ldots,k} : \cdots : x_{n-k+1,\ldots,n}] \in \mathbb{P}^{\binom{n}{k}-1}$. Then there exists a subspace $\mathcal{U} \in \mathcal{G}_q(k,n)$ such that $\varphi(\mathcal{U}) = x$ if and only if*

$$\sum_{j\in\{i_1,\ldots,i_{k+1}\}} \mathrm{sgn}(\sigma_j) x_{i_1,\ldots,i_{k+1}\setminus j} x_{j,i_{k+2},\ldots,i_{2k}} = 0$$

$\forall (i_1,\ldots,i_{k+1}) \in \binom{[n]}{k+1}, (i_{k+2},\ldots,i_{2k}) \in \binom{[n]}{k-1}$, where $\mathrm{sgn}(\sigma_j)$ denotes the sign of the permutation such that

$$\sigma_{i_\ell}(i_1,\ldots,i_{k+1}) = (i_\ell, i_1, \ldots, i_{\ell-1}, i_{\ell+1}, \ldots, i_{k+1}).$$

Then one can easily derive an upper bound on the number of shuffle equations.

Lemma 6 *There are at most $\binom{n}{k+1}\binom{n}{k-1}$ different (non-trivial) shuffle relations defining $\mathcal{G}_q(k,n)$ in the Plücker embedding.*

Example 3 $\mathcal{G}_q(2,4)$ is described by a single relation:

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

3 Balls in the Grassmannian $\mathcal{G}_q(k,n)$

3.1 Description by linear equations in the Plücker embedding

It is known that the equations defining the balls inside $\mathcal{G}_q(k,n)$ around an element from $\mathcal{G}_q(k,n)$ are easily determined in the following special case:

Proposition 7 ([12,21]) *Define* $\mathcal{U}_0 := \mathrm{rs}[\, I_k \; 0_{k\times n-k}\,]$. *Then for* $t \leq k-1$

$$B^k_{S,2t}(\mathcal{U}_0) = \{\mathcal{V} = \mathrm{rs}(V) \in \mathcal{G}_q(k,n) \mid M_{i_1,\ldots,i_k}(V) = 0 \\ \forall (i_1,\ldots,i_k) \not\preceq (t+1,\ldots,k,n-t+1,\ldots,n)\}.$$

Note that for $t = k$ *it holds that* $B^k_{S,2k}(\mathcal{U}) = \mathcal{G}_q(k,n)$ *for any* $\mathcal{U} \in \mathcal{G}_q(k,n)$.

We now want to state a generalization of this fact, where the center of the ball can have a different dimension than k. For this we first need the following lemma.

Lemma 8 *Let* $\mathcal{U},\mathcal{V} \in \mathcal{P}_q(n)$ *with* $\dim(\mathcal{U}) = k$ *and* $\dim(\mathcal{V}) = k'$.

1. *Then* $d_S(\mathcal{U},\mathcal{V})$ *is odd if and only if exactly one of* k *and* k' *is odd. Equivalently* $d_S(\mathcal{U},\mathcal{V})$ *is even if and only if both* k *and* k' *are odd or if both are even.*
2. *It holds that* $k - k' + d_S(\mathcal{U},\mathcal{V})$ *and* $k' - k + d_S(\mathcal{U},\mathcal{V})$ *are always even numbers.*

Proof It holds that $d_S(\mathcal{U},\mathcal{V}) = k + k' - 2\dim(\mathcal{U}\cap\mathcal{V})$, i.e. it is odd if and only if $k+k'$ is odd. This directly implies the first statement. The second statement follows since $k-k'$ and $k'-k$ are odd if and only if exaclty one of k and k' is odd, as well. □

We can now state the generalization of Proposition 7 for the subspace distance.

Theorem 9 *Let* $\mathcal{U}_0^{k'} := \mathrm{rs}[\, I_{k'} \; 0_{k'\times n-k'}\,]$. *Then for* $|k-k'| \leq \tau < \min(k'+k, 2n-(k'+k))$, *s.t.* $\frac{k+k'-\tau}{2} \in \mathbb{Z}$ *(which we can assume because of Lemma 8)*

$$B^k_{S,\tau}(\mathcal{U}_0^{k'}) = \Big\{\mathcal{V} = \mathrm{rs}(V) \in \mathcal{G}_q(k,n) \mid M_{i_1,\ldots,i_k}(V) = 0 \;\forall\, (i_1,\ldots,i_k) \not\preceq \\ \left(\frac{k'-k+\tau}{2}+1,\ldots,k', n-\frac{k-k'+\tau}{2}+1,\ldots,n\right)\Big\}.$$

Proof We want to find all $\mathcal{V} = \mathrm{rs}(V) \in \mathcal{G}_q(k,n)$, such that

$$d_S(\mathcal{U}_0^{k'},\mathcal{V}) \leq \tau$$
$$\iff \dim(\mathcal{U}_0^{k'}\cap\mathcal{V}) \geq \frac{k+k'-\tau}{2}$$

i.e. at least $\frac{k+k'-\tau}{2}$ many linearly independent elements of $\mathcal{V}$ have to be in $\mathcal{U}_0^{k'}$. Thus, we can choose a matrix representation of the form

$$V = \left[\begin{array}{c|c} * & 0_{(\frac{k+k'-\tau}{2})\times(n-k')} \\ \hline * & * \end{array}\right].$$

Each $k\times k$-submatrix of V is then of the form

$$M = \left[\begin{array}{c|c} M_1 & 0_{(\frac{k+k'-\tau}{2})\times x} \\ \hline M_2 & M_3 \end{array}\right]$$

where $0 \leq x \leq k$ is the number of columns taken from the $n-k'$ right most columns of V and M_1 is a $\frac{k+k'-\tau}{2} \times (k-x)$ matrix. Since $\mathrm{rank}(M) \leq \mathrm{rank}(M_1) + \mathrm{rank}([M_2 M_3]) \leq (k-x) + \frac{k-k'+\tau}{2} = k - (x - \frac{k-k'+\tau}{2})$ it follows that all minors of V that contain at least $x = \frac{k-k'+\tau}{2}+1$ of the $n-k'$ rightmost columns are zero. At the same time this is also a sufficient condition, since the $*$-blocks

of V can be filled with anything (such that the whole matrix has rank k) and the row space will always be in the ball. Since the monomials are ordered, the condition that at least $\frac{k-k'+\tau}{2}+1$ many coordinates of $(i_1,\ldots,i_k)$ are in $\{k'+1,\ldots,n\}$ is equivalent to the condition that

$$i_\ell \geq k'+1 \text{ for some } \ell \in \left\{1,\ldots,\frac{k+k'-\tau}{2}\right\}$$

which is in turn equivalent to

$$(i_1,\ldots,i_k) \not\preceq \left(k'-\frac{k+k'-\tau}{2}+1,\ldots,k',n-\frac{k-k'+\tau}{2}+1,\ldots,n\right)$$

$$\iff (i_1,\ldots,i_k) \not\preceq \left(\frac{k'-k+\tau}{2}+1,\ldots,k',n-\frac{k-k'+\tau}{2}+1,\ldots,n\right).$$

□

In analogy, we can also state the generalization of Proposition 7 for the injection distance:

Theorem 10 *Define $\mathcal{U}_0^{k'}$ as before. Then for $|k'-k| \leq t < \min(\max(k',k), n-k+1)$*

$$B_{I,t}^k(\mathcal{U}_0^{k'}) = \Big\{\mathcal{V}=\mathrm{rs}(V)\in\mathcal{G}_q(k,n) \mid M_{i_1,\ldots,i_k}(V)=0 \;\forall\; (i_1,...,i_k) \not\preceq (k'-\max(k',k)+t+1,\ldots,k',n-k+\max(k',k)-t+1,\ldots,n)\Big\}.$$

Proof We want to find all $\mathcal{V}=\mathrm{rs}(V)\in\mathcal{G}_q(k,n)$, such that

$$d_I(\mathcal{U}_0^{k'},\mathcal{V}) \leq t$$

$$\iff \dim(\mathcal{U}_0^{k'}\cap\mathcal{V}) \geq \max(k',k)-t,$$

i.e. at least $\max(k',k)-t$ many linearly independent elements of $\mathcal{V}$ have to be in $\mathcal{U}_0^{k'}$. Thus, we can choose a matrix representation of the form

$$V=\left[\begin{array}{c|c} * & 0_{(\max(k',k)-t)\times(n-k')} \\ * & * \end{array}\right].$$

Analogously to the proof of Theorem 9 this is equivalent to the statement that all minors containing at least $\min(0,k-k')+t+1$ of the $n-k'$ rightmost columns are zero, which is in turn equivalent to

$$(i_1,\ldots,i_k) \not\preceq (k'-\max(k',k)+t+1,\ldots,k',n-k+\max(k',k)-t+1,\ldots,n).$$

□

The following proposition shows that the conditions on τ and t in the previous theorems make sense.

Proposition 11 *Let $\mathcal{U}\in\mathcal{G}_q(k',n)$.*

1. *For $\tau=\min(k'+k,2n-(k'+k))$ it holds that $B_{S,\tau}^k(\mathcal{U})=\mathcal{G}_q(k,n)$.*
2. *For $t=\min(\max(k',k),n-\max(k',k))$ it holds that $B_{I,t}^k(\mathcal{U})=\mathcal{G}_q(k,n)$.*
3. *For $\tau<|k'-k|$ it holds that $B_{S,\tau}^k(\mathcal{U})=B_{I,\tau}^k(\mathcal{U})=\emptyset$.*

Proof Let $\mathcal{V}\in\mathcal{G}_q(k,n)$.

1. Let $\tau=k'+k$. Then $d_S(\mathcal{U},\mathcal{V})=k'+k \iff \dim(\mathcal{U}\cap\mathcal{V})=0 \iff B_{S,k+k'}^k(\mathcal{U})=\mathcal{G}_q(k,n)$.
   Let $\tau=2n-(k+k')$. Since it is known that $d_S(\mathcal{U},\mathcal{V})=d_S(\mathcal{U}^\perp,\mathcal{V}^\perp)$ it holds that

$$B_{S,2n-(k+k')}^k(\mathcal{U})=(B_{S,(n-k)+(n-k')}^{n-k}(\mathcal{U}^\perp))^\perp=\mathcal{G}_q(n-k,k)^\perp=\mathcal{G}_q(k,n).$$

2. Let $t = \max(k', k)$. Then $d_I(\mathcal{U}, \mathcal{V}) = \max(k', k) \iff \dim(\mathcal{U} \cap \mathcal{V}) = 0 \iff B^k_{I,\max(k',k)}(\mathcal{U}) = \mathcal{G}_q(k, n)$.
   Let $t = n - \min(k', k) = \max(n - k', n - k)$. Since it is known that $d_I(\mathcal{U}, \mathcal{V}) = d_I(\mathcal{U}^\perp, \mathcal{V}^\perp)$ it holds that $B^k_{I,n-\min(k',k)}(\mathcal{U}) = (B^{n-k}_{I,\max(n-k',n-k)}(\mathcal{U}^\perp))^\perp = \mathcal{G}_q(n-k, k)^\perp = \mathcal{G}_q(k, n)$.
3. Moreover, $d_S(\mathcal{U}, \mathcal{V}) < |k' - k| \iff d_I(\mathcal{U}, \mathcal{V}) < |k' - k| \iff \dim(\mathcal{U} \cap \mathcal{V}) > \min(k, k') \iff B^k_{S,k+k'}(\mathcal{U}) = B^k_{I,k+k'}(\mathcal{U}) = \emptyset$.

□

Remark 12 The linear equations described in Theorems 9 and 10 together with the shuffle relations described in Proposition 5 show that the balls $B^k_{S,t}(\mathcal{U}_0^{k'})$ as well as the balls $B^k_{I,t}(\mathcal{U}_0^{k'})$ are sub-varieties of the Grassmann variety $\mathcal{G}_q(k, n)$.

Remark 13 In Theorems 9 and 10, for $t = k' - k$ (if $k' \geq k$) the formula for the balls becomes

$$B^k_{S,t}(\mathcal{U}_0^{k'}) = B^k_{I,t}(\mathcal{U}_0^{k'}) = \\ \left\{\mathcal{V} = \mathrm{rs}(V) \in \mathcal{G}_q(k, n) \mid M_{i_1,\ldots,i_k}(V) = 0 \; \forall \; (i_1, ..., i_k) \not\preceq (k' - k + 1, \ldots, k')\right\}.$$

Example 4 1. Consider $\mathcal{G}_q(2, 6)$ and $\mathcal{U}_0^3 = \mathrm{rs}\begin{pmatrix} 1&0&0&0&0&0 \\ 0&1&0&0&0&0 \\ 0&0&1&0&0&0 \end{pmatrix}$. Then $k = 2, k' = 3$ and

$$B^2_{S,3}(\mathcal{U}_0^3) = B^2_{S,2}(\mathcal{U}_0^3) = \{\mathcal{V} = \mathrm{rs}(V) \in \mathcal{G}_q(2, 6) \mid M_{i_1,i_2}(V) = 0 \forall (i_1, i_2) \not\preceq (3, 6)\}.$$

2. Consider $\mathcal{G}_q(3, 6)$ and $\mathcal{U}_0^2 = \mathrm{rs}\begin{pmatrix} 1&0&0&0&0&0 \\ 0&1&0&0&0&0 \end{pmatrix}$. Then $k = 3, k' = 2$ and

$$B^3_{S,3}(\mathcal{U}_0^2) = B^3_{I,2}(\mathcal{U}_0^2) = \{\mathcal{V} = \mathrm{rs}(V) \in \mathcal{G}_q(3, 6) \mid M_{i_1,i_2,i_3}(V) = 0 \forall (i_1, i_2, i_3) \not\preceq (2, 5, 6)\}.$$

We can find a relation for the balls of the two different metrics as follows.

Proposition 14 *Let $\mathcal{U} \in \mathcal{G}_q(k', n)$ and $\mathcal{V} \in \mathcal{G}_q(k, n)$. Then*

$$d_S(\mathcal{U}, \mathcal{V}) = 2d_I(\mathcal{U}, \mathcal{V}) + k + k' - 2\max(k', k)$$

and

$$B_{I,t}(\mathcal{U}) = B_{S,2t+k+k'-2\max(k',k)}(\mathcal{U}).$$

Proof First, it holds that

$$\begin{aligned} 2d_I(\mathcal{U}, \mathcal{V}) + k + k' - 2\max(k', k) &= 2\max(k', k) - 2\dim(\mathcal{U} \cap \mathcal{V}) + k + k' - 2\max(k', k) \\ &= k + k' - 2\dim(\mathcal{U} \cap \mathcal{V}) = d_S(\mathcal{U}, \mathcal{V}) \end{aligned}$$

Second, it holds that

$$\begin{aligned} &\mathcal{V} \in B_{S,2t+k+k'-2\max(k',k)}(\mathcal{U}) \iff d_S(\mathcal{U}, \mathcal{V}) \leq 2t + k + k' - 2\max(k', k) \\ \iff\; & k + k' - 2\dim(\mathcal{U} \cap \mathcal{V}) \leq 2t + k + k' - 2\max(k', k) \iff \dim(\mathcal{U} \cap \mathcal{V}) \geq \max(k', k) - t \\ \iff\; & \max(k', k) - \dim(\mathcal{U} \cap \mathcal{V}) \leq t \iff d_I(\mathcal{U}, \mathcal{V}) \leq t \iff \mathcal{V} \in B_{I,t}(\mathcal{U}). \end{aligned}$$

□

With the knowledge of $B^k_{S,\tau}(\mathcal{U}_0^{k'})$ we can also express $B^k_{S,\tau}(\mathcal{U})$ for any $\mathcal{U} \in \mathcal{G}_q(k', n)$. To do so we need the following result.

Lemma 15 *For any $\mathcal{U} \in \mathcal{G}_q(k', n)$ there exists an $A \in GL_n$ such that $\mathcal{U}_0^{k'} A = \mathcal{U}$. Moreover,*

$$B^k_{S,\tau}(\mathcal{U}_0^{k'} A) = B^k_{S,\tau}(\mathcal{U}_0^{k'})A.$$

The same holds for the injection distance, i.e.

$$B^k_{I,\tau}(\mathcal{U}_0^{k'} A) = B^k_{I,\tau}(\mathcal{U}_0^{k'})A.$$

Proof Both statements follow from the fact that $\dim(\mathcal{U}_0^{k'} A \cap \mathcal{V}) = \dim(\mathcal{U}_0^{k'} \cap \mathcal{V}A^{-1})$, since this directly implies that $d_S(\mathcal{U}_0^{k'} A, \mathcal{V}) \leq \tau \iff d_S(\mathcal{U}_0^{k'}, \mathcal{V}A^{-1})$ and $d_I(\mathcal{U}_0^{k'} A, \mathcal{V}) \leq \tau \iff d_I(\mathcal{U}_0^{k'}, \mathcal{V}A^{-1})$. □

Remark 16 Note that one can easily find $A \in GL_n$ such that $\mathcal{U}_0^{k'} A = \mathcal{U}$ as follows: Let the upper k' rows of A be equal to the reduced row echelon form of $\mathcal{U}$ and fill the lower rows with unit vectors such that the respective ones and the pivots of the upper rows are all in different columns. This implies that A is invertible and that $\mathcal{U}_0^{k'} A = \mathcal{U}$. For an algorithmic description of constructing such an A see [21,31].

The following results are generalizations of results from [21]. For simplifying the computations we define $\bar{\varphi}$ on GL_n, where we denote by $A_{j_1,\ldots,j_k}[i_1,\ldots,i_k]$ the submatrix of A that consists of the rows $i_1,\ldots,i_k$ and columns $j_1,\ldots,j_k$:

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

Lemma 17 ([21]) *Let $\mathcal{U} \in \mathcal{G}_q(k,n)$ and $A \in GL_n$. It holds that*

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

Since it holds for any k, we can use this lemma to describe a ball around a subspace of arbitrary dimension.

Corollary 18 *Let $\mathcal{U} = \mathcal{U}_0^{k'} A \in \mathcal{G}_q(k',n)$. Then*

$$\begin{aligned} B_{S,\tau}^k(\mathcal{U}) = B_{S,\tau}^k(\mathcal{U}_0^{k'} A) = \Big\{ &\mathcal{V} = \mathrm{rs}(V) \in \mathcal{G}_q(k,n) \mid M_{i_1,\ldots,i_k}(V)\bar{\varphi}(A^{-1}) = 0 \ \forall (i_1,\ldots,i_k) \not\preceq \\ &\left(\frac{k'-k+\tau}{2}+1,\ldots,k', n-\frac{k-k'+\tau}{2}+1,\ldots,n\right)\Big\}, \\ B_{I,t}^k(\mathcal{U}) = B_{I,t}^k(\mathcal{U}_0^{k'} A) = \Big\{ &\mathcal{V} = \mathrm{rs}(V) \in \mathcal{G}_q(k,n) \mid M_{i_1,\ldots,i_k}(V)\bar{\varphi}(A^{-1}) = 0 \ \forall (i_1,\ldots,i_k) \not\preceq \\ &(k'-\max(k',k)+t+1,\ldots,k', n-k+\max(k',k)-t+1,\ldots,n)\Big\}. \end{aligned}$$

In the following we calculate the number of equations which define a ball of a given radius.

Lemma 19 *The maximum number of linear Plücker equations defining a ball $B_{S,\tau}^k(\mathcal{U}_0^{k'})$ (respectively $B_{I,t}^k(\mathcal{U}_0^{k'})$) is equal to the maximum number of equations defining $B_{S,\tau}^k(\mathcal{U})$ (respectively $B_{I,t}^k(\mathcal{U})$) for any $\mathcal{U} \in \mathcal{G}_q(k',n)$.*

Proof Follows directly from Corollary 18. □

We can hence count the maximum number of linear equations needed to describe the ball inside the Grassmannian.

Lemma 20 *Let $\mathcal{U} \in \mathcal{G}_q(k,n)$. An upper bound on the number of linear equations needed to describe $B_{S,\tau}^k(\mathcal{U})$ is*

$$\theta_S := \sum_{l=0}^{\frac{k+k'-\tau}{2}-1} \binom{n-k'}{k-\ell}\binom{k'}{\ell}.$$

An upper bound on the number of linear equations needed to describe $B_{I,t}^k(\mathcal{U})$ is

$$\theta_I := \sum_{l=0}^{\max(k',k)-t-1} \binom{n-k'}{k-\ell}\binom{k'}{\ell}.$$

Proof Follows from Lemma 19 and Theorems 9 and 10. □

Note that all these equations defining a ball (in subspace or injection metric) are linearly independent. This can be seen by the description of the balls around $\mathcal{U}_0^{k'}$, since the equations are of the form $M_{i_1,\dots,i_k}(V) = 0$ for different minors functioning as the variables and are thus linearly independent. As the equations describing the balls around arbitrary elements can be found by linear transformations, also these equations will also be linearly independent.

3.2 Description by rational parametrization

One can also use a rational parametrization to describe the balls around $\mathcal{U}_0^{k'}$ in the Grassmannian as follows.

Proposition 21 *Define $\mathcal{U}_0^{k'}$ as previously and $\nu := \frac{k-k'+\tau}{2}, \omega := \min(0, k-k') + t$. Then*

$$B_{S,\tau}^k(\mathcal{U}_0^{k'}) = \Big\{ \mathcal{V} = \mathrm{rs}[V_1\ V_2] \in \mathcal{G}_q(k,n) \quad | \, V_1 \in \mathbb{F}_q^{k\times k'}, \exists X \in \mathbb{F}_q^{k\times\nu}, Y \in \mathbb{F}_q^{\nu\times(n-k')} : V_2 = XY \Big\}$$

and

$$B_{I,t}^k(\mathcal{U}_0^{k'}) = \Big\{ \mathcal{V} = \mathrm{rs}[V_1\ V_2] \in \mathcal{G}_q(k,n) \quad | \, V_1 \in \mathbb{F}_q^{k\times k'}, \exists X \in \mathbb{F}_q^{k\times\omega}, Y \in \mathbb{F}_q^{\omega\times(n-k')} : V_2 = XY \Big\}.$$

Proof We want to find all $\mathcal{V} = \mathrm{rs}[V_1\ V_2] \in \mathcal{G}_q(k,n)$ such that

$$d_S(\mathcal{U}_0^{k'}, \mathcal{V}) \le \tau \iff \mathrm{rank} \begin{bmatrix} I_{k'} & 0_{k'\times(n-k')} \\ V_1 & V_2 \end{bmatrix} \le \frac{k+k'+\tau}{2}$$

$$\iff k' + \mathrm{rank}(V_2) \le \frac{k+k'+\tau}{2} \iff \mathrm{rank}(V_2) \le \nu.$$

The last statement is equivalent to the fact that there exists $X \in \mathbb{F}_q^{k\times\nu}, Y \in \mathbb{F}_q^{\nu\times(n-k')}$ such that $V_2 = XY$. The proof for the injection distance is analogous. □

Remark 22 As the proof shows for the description of the balls $B_{S,\tau}^k$ and $B_{I,t}^k$ it is crucial to describe all $k \times m$ matrices V_2 whose rank is at most ν. The set of all $k \times m$ matrices of rank at most ν is sometimes called a *determinantal variety* $D_\nu^{k\times m}$. These varieties are known to be rational, this means there is a birational isomorphism from a Zariski open subset of this variety to an open subset of a vector space. To make this concrete in our setting identify the set of all $k \times \nu$ matrices $X = \begin{bmatrix} X_1 \\ X_2 \end{bmatrix}$, where the top part X_1 is an invertible matrix, with an open subset of the vector space $\mathbb{F}^{k\nu}$. Similarly identify the set of $\nu \times m$ matrices having the form $Y = [I_\nu\ Y_2]$ with the vector space $\mathbb{F}^{\nu\times(m-\nu)}$. Then

$$\begin{aligned} f : \mathbb{F}_q^{k\nu} \times \mathbb{F}_q^{\nu\times(m-\nu)} &\longrightarrow D_\nu^{k\times m} \\ (X, Y) &\longmapsto XY \end{aligned}$$

defines a birational isomorphism. The map in particular provides a "rational parametrization" of the variety $D_\nu^{k\times m}$ and in particular the dimension of $D_\nu^{k\times m}$ is equal to $k\nu + m\nu - \nu^2$. Note that not all points of the variety $D_\nu^{k\times m}$ are parametrized but the description avoids dealing with many equations describing the vanishing of the $(\nu+1) \times (\nu+1)$ minors.

In analogy to Section 3.1 we can also describe the balls around arbitrary elements in $\mathcal{G}_q(k,n)$ in a similar manner.

Theorem 23 *Let $\mathcal{R} = \mathrm{rs}[\ R_1\ R_2\ ] \in \mathcal{G}_q(k', n)$ such that $R_1 \in \mathbb{F}_q^{k' \times k'}, R_2 \in \mathbb{F}_q^{k' \times (n-k')}$. Moreover, let ν and ω be as before. Then there exists*

$$A = \left(\begin{array}{c|c} R_1 & R_2 \\ \hline R_3 & R_4 \end{array}\right) \quad \in \mathrm{GL}_n$$

such that $\mathcal{R} = \mathrm{rs}[I_{k'}\ 0_{k' \times (n-k')}]A$. It holds that

$$B^k_{S,\tau}(\mathcal{R}) = \Big\{ \mathcal{V} = \mathrm{rs}\left([V_1 + V_2] \begin{bmatrix} R_1 & R_2 \\ R_3 & R_4 \end{bmatrix} \right) \in \mathcal{G}_q(k,n) \mid V_1 \in \mathbb{F}_q^{k \times k'}, \exists X \in \mathbb{F}_q^{k \times \nu}, Y \in \mathbb{F}_q^{\nu \times (n-k')} : V_2 = XY \Big\}$$

and

$$B^k_{I,t}(\mathcal{R}) = \Big\{ \mathcal{V} = \mathrm{rs}[\ V_1R_1 + V_2R_3 \quad V_1R_2 + V_2R_4\ ] \in \mathcal{G}_q(k,n) \mid V_1 \in \mathbb{F}_q^{k \times k'}, \exists X \in \mathbb{F}_q^{k \times \omega}, Y \in \mathbb{F}_q^{\omega \times (n-k')} : V_2 = XY \Big\}.$$

Proof We know from Lemma 15 that $B^k_{S,\tau}(\mathcal{R}) = B^k_{S,\tau}(\mathcal{U}_0^{k'})A$. Together with Proposition 21 it follows that

$$\begin{aligned} B^k_{S,\tau}(\mathcal{R}) &= \Big\{ \mathcal{V} = \mathrm{rs}[\ V_1\ V_2\ ]A \in \mathcal{G}_q(k,n) \mid V_1 \in \mathbb{F}_q^{k \times k'}, \exists X \in \mathbb{F}_q^{k \times \nu}, Y \in \mathbb{F}_q^{\nu \times (n-k')} : V_2 = XY \Big\} \\ &= \Big\{ \mathcal{V} = \mathrm{rs}[\ V_1R_1 + V_2R_3 \quad V_1R_2 + V_2R_4\ ] \in \mathcal{G}_q(k,n) \mid \\ &\qquad V_1 \in \mathbb{F}_q^{k \times k'}, \exists X \in \mathbb{F}_q^{k \times \nu}, Y \in \mathbb{F}_q^{\nu \times (n-k')} : V_2 = XY \Big\}. \end{aligned}$$

The proof for the injection distance is analogous. □

Corollary 24 *In the setting of Theorem 23, if R_1 has full rank, one can choose a matrix representation of the form $\mathcal{R} = [I_{k'}\ \tilde{R}_2]$. Then the formulas are simplified to*

$$B^k_{S,\tau}(\mathcal{R}) = \Big\{ \mathcal{V} = \mathrm{rs}[\ V_1 \quad V_1\tilde{R}_2 + V_2\ ] \in \mathcal{G}_q(k,n) \mid V_1 \in \mathbb{F}_q^{k \times k'}, \exists X \in \mathbb{F}_q^{k \times \nu}, Y \in \mathbb{F}_q^{\nu \times (n-k')} : V_2 = XY \Big\}$$

and

$$B^k_{I,t}(\mathcal{R}) = \Big\{ \mathcal{V} = \mathrm{rs}[\ V_1 \quad V_1\tilde{R}_2 + V_2\ ] \in \mathcal{G}_q(k,n) \mid V_1 \in \mathbb{F}_q^{k \times k'}, \exists X \in \mathbb{F}_q^{k \times \omega}, Y \in \mathbb{F}_q^{\omega \times (n-k')} : V_2 = XY \Big\}.$$

Proof Because of the shape of $\mathcal{R}$ we can choose

$$A = \begin{pmatrix} I_{k'} & \tilde{R}_2 \\ 0 & I_{n-k'} \end{pmatrix}$$

such that $\mathrm{rs}[\ I_{k'}\ 0\ ]A = \mathrm{rs}[\ R_1\ R_2\ ]$. Then the statement follows from Theorem 23. □

Example 5 Consider $\mathcal{G}_q(2,4)$ and let $\mathcal{R} = \mathrm{rs}\begin{pmatrix} 1&0&0&1 \\ 0&1&1&1 \end{pmatrix}$. Then $k = k' = 2$ and

$$\begin{aligned} &B^2_{S,2}(\mathcal{R}) = \\ &\Big\{ \mathrm{rs}\left[V_1 \ \ V_1 \begin{pmatrix} 0&1 \\ 1&1 \end{pmatrix} + V_2 \right] \in \mathcal{G}_q(2,4) \mid V_1 \in \mathbb{F}_q^{2\times 2}, \quad V_2 = (X_1X_2)^T(Y_1Y_2), \quad X_1, X_2, Y_1, Y_2 \in \mathbb{F}_q \Big\} \\ &\qquad = \Big\{ \mathrm{rs}\begin{pmatrix} a & b & b + X_1Y_1 & a + b + X_1Y_2 \\ c & d & d + X_2Y_1 & c + d + X_2Y_2 \end{pmatrix} \in \mathcal{G}_q(2,4) \mid a,b,c,d,X_1,X_2,Y_1,Y_2 \in \mathbb{F}_q \Big\}. \end{aligned}$$

In the description of the balls from Theorem 23, define $\bar{V} := V_1R_1 + V_2R_3$ (i.e. the left part of the elements in the ball) and $\tilde{V} := V_1R_2 + V_2R_4$ (i.e. the right part of the elements in the ball). Then for a given R_2 and some $V_1 \in \mathbb{F}_q^{k\times k}$ one gets a set of bilinear equations of the form

$$\bar{V}_{ij} = \sum_{\ell=1}^{k'}(V_1)_{i\ell}(R_1)_{\ell j} + \sum_{\ell=1}^{n-k'}\sum_{m=1}^{\nu} X_{im}Y_{m\ell}(R_3)_{\ell j}$$

$$\tilde{V}_{ij} = \sum_{\ell=1}^{k'}(V_1)_{i\ell}(R_2)_{\ell j} + \sum_{\ell=1}^{n-k'}\sum_{m=1}^{\nu} X_{im}Y_{m\ell}(R_4)_{\ell j}$$

for the subspace distance and of the form

$$\bar{V}_{ij} = \sum_{\ell=1}^{k'}(V_1)_{i\ell}(R_1)_{\ell j} + \sum_{\ell=1}^{n-k'}\sum_{m=1}^{\omega} X_{im}Y_{m\ell}(R_3)_{\ell j}$$

$$\tilde{V}_{ij} = \sum_{\ell=1}^{k'}(V_1)_{i\ell}(R_2)_{\ell j} + \sum_{\ell=1}^{n-k'}\sum_{m=1}^{\omega} X_{im}Y_{m\ell}(R_4)_{\ell j}$$

for the injection distance. From this we can determine the degree and the number of variables of this system of equations:

Lemma 25 *For a given V_1, the description of the balls from Theorem 23 results in a system of bilinear equations in $kk' + (n - k' + k)\nu$ unknowns for the subspace distance, respectively $kk' + (n - k' + k)\omega$ unknowns for the injection distance, given by V_1, X and Y.*

To sum up, we know how to describe the balls, in both the subspace and the injection metric, in $\mathcal{G}_q(k, n)$ with a given radius around an element of $\mathcal{P}_q(n)$ with either linear equations in the Plücker embedding or bilinear equations in the matrix coordinates. In the following sections we will show how this can be used to establish list decoding algorithms for lifted Gabidulin codes.

4 Lifted Gabidulin Codes

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

$$d_R(A, B) := \operatorname{rank}(A - B) \ .$$

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 [3,7,22] that

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

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 [7]. 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 $g_i \in \mathbb{F}_{q^\ell}$, $1 \leq i \leq k$, be linearly independent over $\mathbb{F}_q$. Then the generator matrix G of a $[k \times \ell, \varrho, \delta]$ Gabidulin MRD code is given by

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

where $\varrho = \ell(k-\delta+1)$, and $[i] = q^i$ [7].

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 [25].

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 code*.

Theorem 26 ([25]) *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.*

We will now show that the row expansion of a Gabidulin code forms a linear block code. Let C be an $[k \times \ell, \ell(k-\delta+1), \delta)]$ Gabidulin MRD code over $\mathbb{F}_q$, $k \leq \ell$. We denote by C^L the linear block code of length $k\ell$ over $\mathbb{F}_q$, such that every codeword c^A of C^L is obtained from a codeword $A \in C$ by taking the entries of A, row by row, from bottom to top, left to right (w.l.o.g.).

Theorem 27 *The code C^L is a $[k\ell, \ell(k-\delta+1), \geq \delta]$ linear block code over $\mathbb{F}_q$ in the Hamming metric.*

Proof The linearity of C^L directly follows from the linearity of C. The length of C^L is the number of entries in a codeword of C, and C and C^L have the same cardinality. 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^L satisfies $d_{min} \geq \delta$. □

We denote by H^L a parity-check matrix of C^L.

We will now show that also a subset of the Plücker coordinates of a lifted Gabidulin code is a linear block code over F_q.

As before, let C be an $[k \times (n-k), (n-k)(k-\delta+1, \delta)]$ Gabidulin MRD code over $\mathbb{F}_q$. Then by Theorem 26 its lifting is a code $\mathcal{C}$ of size $q^{(n-k)(k-\delta+1)}$ in the Grassmannian $\mathcal{G}_q(k,n)$. Let

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

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 $x^{\mathcal{A}}_{1\ldots k} = 1$ for any $\mathcal{A} \in \mathcal{C}$.

Let $[k] = \{1, 2, \ldots, k\}$, and let $\underline{i} = \{i_1, i_2, \ldots, i_k\}$ 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 28 *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.

Similarly to Theorem 27, with Lemma 28 one can easily show, that a subset of the Plücker coordinates of a lifted Gabidulin code forms a linear code over $\mathbb{F}_q$:

Theorem 29 *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 Hamming distance $d_{min} \geq \delta$.*

Remark 30 When $\mathbb{F}_q = \mathbb{F}_2$, then C^p is equivalent to C^L.

We denote by H^p a parity-check matrix of C^p.

Example 6 Let $\alpha \in \mathbb{F}_{2^2}$ be a primitive element, fulfilling $\alpha^2 = \alpha + 1$. Let C be the $[2 \times 2, 2, \delta = 2]$ Gabidulin MRD code over $\mathbb{F}_2$ defined by the generator matrix $G = (\alpha\ 1)$. In this example we want to consider the lifting of $C = \{(b\alpha, b) : b \in \mathbb{F}_{2^2}\}$. 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
$(0,0)$	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$	$\mathrm{rs}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$	$[1:0:0:0:0:0]$
$(\alpha,1)$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\mathrm{rs}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$	$[1:1:0:0:1:1]$
(α^2,α)	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$	$[1:0:1:1:1:1]$
$(1,\alpha^2)$	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	$\mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$	$[1:1:1:1:0:1]$

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 $x_{13} + x_{23} + x_{24} = 0$.

5 List Decoding of Lifted Gabidulin Codes

We now have all the machinery needed to describe two list decoding algorithms for lifted Gabidulin codes, one in the Plücker coordinates and another one in the matrix entries. We will describe everything in this section using the subspace distance. The translation of these results to the injection metric is then straight-forward. In this section we will describe both list decoding algorithms and give a bound on the list size for lifted Gabidulin codes.

5.1 List decoding in the Plücker embedding

Consider a lifted Gabidulin 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.

We showed in Section 4 how a subset of the Plücker coordinates of a lifted Gabidulin 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 $[x_{1\ldots k} : \ldots : x_{n-k+1\ldots n}]\bar{H^p}^T = 0$ gives rise to the same equations as $[x_{i_1} : \ldots : x_{i_{k(n-k)}}]H^{pT} = 0$, for $i_1, \ldots, i_{k(n-k)} \in \underline{i}$. For simplicity we will write $\bar{x}$ for $[x_{1\ldots k} : \ldots : x_{n-k+1\ldots n}]$ in the following.

Lemma 31 *The linear equations $\bar{x}\bar{H^p}^T = 0$ together with the normalization condition $x_{1,\ldots,k} = 1$ and the shuffle relations described in Proposition 5 describe the lifted Gabidulin code $\mathcal{C}$ in terms of its Plücker coordinates.*

Remark 32 Using the language of algebraic geometry one can also say that $\mathcal{C}$ has the structure of a quasi-projective sub-variety of the Grassmann variety $\mathcal{G}_q(k,n)$.

The list decoding problem up to the decoding radius τ requires the explicit description of the intersection of the varieties

$$L^{\tau}_{\mathcal{C}}(\mathcal{R}) := \mathcal{C} \cap B^k_{S,\tau}(\mathcal{R}),$$

which we will call the *list variety* of the received subspace $\mathcal{R}$. The following algorithm provides an explicit computation of the equations describing $L^{\tau}_{\mathcal{C}}(\mathcal{R})$.

Algorithm 1

Input: received word $\mathcal{R} \in \mathcal{P}_q(n)$, decoding radius τ

1. Find the (linear) equations defining $B^k_{S,\tau}(\mathcal{R})$ in the Plücker coordinates, as explained in Section 3.
2. Solve the system of (linear) equations, that arises from $\bar{x}\bar{H^p}^T = 0$, together with the equations of $B^k_{S,\tau}(\mathcal{R})$, the (bilinear) shuffle relations and the equation $x_{1,\ldots,k} = 1$ (describing the lifting).

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

Note that there exist many algorithms to solve bilinear equations that one can use in Step 2. of the algorithm, see e.g. [2,13,27]. In this paper we will consider the relinearization algorithm from [13].

Theorem 33 *Algorithm 1 outputs the complete list L of codewords (in Plücker coordinate representation), such that for each element $\bar{x} \in L$, $d_S(\varphi^{-1}(\bar{x}), \mathcal{R}) \leq \tau$.*

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 $x_{1,\ldots,k} = 1$ 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 $B^k_{S,\tau}(\mathcal{R})$ is then given by the additional equations from Step 1 in the algorithm. Thus the solution set to the whole system of equation is the Plücker equations of $\mathcal{C} \cap B^k_{S,\tau}(\mathcal{R})$. □

Example 7 We consider the $(4,4,4,2)_2$ lifted Gabidulin code from Example 6. Note, that for a received space of dimension 2 it is not possible to decode always to a unique closest codeword.

1. Assume we received

$$\mathcal{R}_1 = \mathrm{rs}\begin{pmatrix} 1&0&1&0 \\ 0&0&0&1 \end{pmatrix}.$$

We would like to correct one error. We first find the equations for the ball of subspace radius 2:

$$B^2_{S,2}(\mathcal{U}_0) = \{\mathcal{V} = \mathrm{rs}(V) \in \mathcal{G}_2(2,4) \mid M_{3,4}(V) = 0\}$$

We construct

$$A_1^{-1} = \begin{pmatrix} 1&0&0&1 \\ 0&0&1&0 \\ 0&0&0&1 \\ 0&1&0&0 \end{pmatrix}$$

(see Remark 16) and compute the last column of $\bar{\varphi}(A_1^{-1})$:

$$[1:0:0:1:0:0]^T.$$

Thus, by Corollary 18 we get that

$$B^2_{S,2}(\mathcal{R}_1) = \{\mathcal{V} = \mathrm{rs}(V) \in \mathcal{G}_2(2,4) \mid M_{1,4}(V) + M_{2,3}(V) = 0\}.$$

Then combining with the parity check equations from Example 6 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 $B^2_{S,2}(\mathcal{R}_1)$ and the last one represents the identity submatrix. 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 6) 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

$$\mathrm{rs}\begin{pmatrix} 1&0&1&0 \\ 0&1&1&1 \end{pmatrix}, \mathrm{rs}\begin{pmatrix} 1&0&1&1 \\ 0&1&0&1 \end{pmatrix}.$$

2. Now assume we received

$$\mathcal{R}_2 = \mathrm{rs}\begin{pmatrix} 1&0&0&1 \\ 0&1&1&1 \end{pmatrix}.$$

As previously, we construct

$$A_2^{-1} = \begin{pmatrix} 1&0&0&1 \\ 0&1&1&1 \\ 0&0&1&0 \\ 0&0&0&1 \end{pmatrix}$$

(see Remark 16) and compute the last column of $\bar{\varphi}(A_2^{-1})$:

$$[1:1:0:1:1:1]^T.$$

Thus, by Corollary 18 we get that

$$B^2_{S,2}(\mathcal{R}_1) = \{\mathcal{V} = \mathrm{rs}(V) \in \mathcal{G}_2(2,4) \mid M_{1,2}(V) + M_{1,3}(V) + M_{2,3}(V) + M_{2,4}(V) + M_{3,4}(V) = 0\}.$$

Then combining with the parity check equations from Example 6 and the shuffle relation from Example 3 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 the 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

$$\mathrm{rs}\begin{pmatrix}1&0&0&1\\0&1&1&0\end{pmatrix}, \mathrm{rs}\begin{pmatrix}1&0&1&1\\0&1&0&1\end{pmatrix}, \mathrm{rs}\begin{pmatrix}1&0&1&0\\0&1&1&1\end{pmatrix}.$$

Remark 34 In the previous example, for the same code and two received words of the same dimension, in one case we needed the bilinear shuffle relations whereas in the other case we could completely list decode without taking the shuffle relations into account. Thus, the actual shape of the received space can make a difference for the complexity of the decoding algorithm.

The complexity of Algorithm 1 is dominated by solving the system of $\theta_S + 1 + (\delta-1)(n-k) + \binom{n}{k-1}\binom{n}{k+1}$ linear and bilinear equations in $\binom{n}{k}$ variables.

Theorem 35 *Using the relinearization algorithm from [13], the complexity of Algorithm 1 is polynomial in n and exponential in k.*

Proof We can use the relinearization algorithm of [13] to solve the system of linear and bilinear equations in Algorithm 1. This algorithm is polynomial in the number of variables if the number of equations is at least the square of the number of variables, which is satisfied in our case, since $\binom{n}{k-1}\binom{n}{k+1} \approx \binom{n}{k}^2$. With the approximation $\binom{n}{k} \approx n^k$, the statement follows. □

Note that it is not easy to determine the actual complexity of the relinearization algorithm as described in [13]. The paper states that the number of arithmetic operations is a polynomial $\psi(N)$ where N is the number of variables involved. For our situation that would translate that the number of arithmetic operations is $O\left(\psi(n^{2k})\right)$ once k is small in comparison to n.

5.2 List decoding with the rational parametrization

We can use the description of the balls from Section 3.2 with the additional constraints from the description of the lifted Gabidulin codes, i.e. the first $k \times k$-block is the identity and the rightmost $n-k$ columns fulfill the parity check equations from the linear code description.

Algorithm 2

Input: received word $\mathcal{R} \in \mathcal{P}_q(n)$, decoding radius τ

1. Find the (bilinear) equations defining $B^k_{S,\tau}(\mathcal{R})$ in the rational parametrization, as explained in Section 3.2.
2. Solve the system of (linear) equations, that arises from H^L, together with the equations of $B^k_{S,\tau}(\mathcal{R})$ and the equations corresponding to the first block of the codewords being equal to the identity. (In the notation of Theorem 23 the variables are given by the matrices V_1, X and Y.)
3. For each solution from 2. compute $U = [\ V_1R_1 + V_2R_3 \quad V_1R_2 + V_2R_4\ ]$ (in the notation of Theorem 23).

Output: matrices U, whose row spaces are the codewords in $B^k_{S,\tau}(\mathcal{R}) \cap \mathcal{C}$.

Example 8 1. Consider $\mathcal{G}_2(2,4)$ and the code from Example 6. Let the received word be $\mathcal{R} = \mathrm{rs}\begin{pmatrix}1&0&0&1\\0&1&1&1\end{pmatrix}$, as in Example 7.2 Then we know from Example 5 that

$$B^2_{S,2}(\mathcal{R}) = \left\{ \mathrm{rs}\begin{pmatrix} a & b & b+X_1Y_1 & a+b+X_1Y_2 \\ c & d & d+X_2Y_1 & c+d+X_2Y_2 \end{pmatrix} \in \mathcal{G}_q(k,n) \mid a,b,c,d,X_1,X_2,Y_1,Y_2 \in \mathbb{F}_q \right\}.$$

Since we want to find only codewords of the lifted Gabidulin code in the ball, we can set $a = d = 1$ and $b = c = 0$. We label the entries of the third and fourth column from bottom left to top right by $(v_1, \ldots, v_4) = (1 + X_2Y_1, 1 + X_2Y_2, X_1Y_1, 1 + X_1Y_2)$. With the parity-check equations from the code C^L (which is the same as C^P in this case)

$$v_1 + v_3 + v_4 = 0 \quad v_2 + v_3 = 0$$

we get the following system of equations:

$$(1 + X_2Y_1) + (1 + X_1Y_1) + (1 + X_1Y_2) = 0 \quad (1 + X_2Y_2) + X_1Y_1 = 0$$

which has the following solutions:

$$(X_1, X_2, Y_1, Y_2) \in \{(0, 1, 0, 1), (1, 0, 1, 1), (1, 1, 1, 0)\}.$$

These correspond to the codewords (remember that one has to add $a = d = 1$ in some coordinates)

$$\mathrm{rs}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

2. Consider the same setting as before but let the received word be $\mathcal{R} = \mathrm{rs}\begin{pmatrix} 0 & 1 & 1 & 1 \end{pmatrix}$. Then we can choose

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

such that $(1000)A = (0111)$ and get by Theorem 23

$$B^2_{S,1}(\mathcal{R}) = \left\{ \mathrm{rs}\begin{pmatrix} X_1Y_1 & a & a + X_1Y_2 & a + X_1Y_3 \\ X_2Y_1 & b & b + X_2Y_2 & b + X_2Y_3 \end{pmatrix} \in \mathcal{G}_q(k, n) \mid a, b, X_1, X_2, X_3, Y_1, Y_2, Y_3 \in \mathbb{F}_q \right\}.$$

Since we want to find only codewords in the ball, we can set $a = 0$ and $b = 1$ and get the constraints $X_1Y_1 = 1, X_2Y_1 = 0$. With the equations from the code we get the following system of equations:

$$X_1Y_1 = 1 \quad X_2Y_1 = 0$$
$$X_1Y_2 + X_2Y_3 = 1 \quad X_1Y_2 + X_1Y_3 + X_2Y_2 = 1$$

which has the unique solution

$$(X_1, X_2, Y_1, Y_2, Y_3) = (1, 0, 1, 1, 0).$$

This corresponds to the codeword (remember that one has to add $b = 1$ in some coordinates)

$$\mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

We can do the following complexity analysis for Algorithm 2.

Theorem 36 *Using the relinearization algorithm from [13], Algorithm 2 has a computational complexity that is polynomial in n and exponential in k (if the list size is small enough).*

Proof We know from Lemma 25 that the system of bilinear equations to be solved in the algorithm has $kk' + n\frac{k-k'+\tau}{2}$ variables, which we can approximate by $kk' + n\frac{\tau}{2}$, if we assume $k \approx k'$. Moreover, it has at most k^2 equations for the identity part and $(n-k)(\delta-1)$ equations for the linear Gabidulin code description (see Theorem 29). Since $\delta \leq k$ we can upper bound the number of equations by $(n-k)k + k^2 = nk$. We now use the relinearization algorithm for solving the system of equations. In this algorithm, either the second linearization has a unique solution or it has a solution space of dimension that is polynomial in k. Then we have to do the last steps for finding the solutions of the original variables for any of the elements of this solution space.

Since the whole relinearization algorithm is polynomial if there is only one solution to the second linearization (see [13]), our algorithm will have at most a complexity that is exponential in k. □

Note, that if one is interested to get a list of codewords of a certain distance of the received word explicitly, then the efficiency of a decoding algorithm depends (at least) on the size of the list. In other words, if there is a list of an exponential size, no polynomial time algorithm can exist which explicitly outputs the total list. From an application point of view the list size is also important, since usually one wants to have a small list size to have sensible list decoding. This is due to the fact that one wants to choose one codeword of the output list after decoding to be the most likely sent codeword. Hence, we investigate the worst possible list sizes in the following.

We will derive a lower bound on the worst case list size for lifted Gabidulin codes in analogy to the theorems and proofs of [34], where these bounds were derived for classical Gabidulin codes. We denote such a worst case list size, i.e. the maximum number of codewords of an $(n, q^{(n-k)(k-\delta+1)}, 2\delta, k)_q$ lifted Gabidulin code $\mathcal{C}$ in a ball of a subspace radius τ around any received word, by $L_S(\tau, n, k, \delta, q)$, and for injection radius t by $L_I(t, n, k, \delta, q)$.

Theorem 37 *Lower bounds on the list sizes $L_S(\tau, n, k, \delta, q)$ and $L_I(t, n, k, \delta, q)$, for $t, \tau/2 < \delta \leq k \leq n/2$, are given by*

$$L_S(\tau, n, k, \delta, q) \geq \frac{\begin{bmatrix} k \\ \lfloor \tau/2 \rfloor \end{bmatrix}_q}{q^{(n-k)(\delta-\lfloor \tau/2 \rfloor-1)}} \quad \text{and} \quad L_I(t, n, k, \delta, q) \geq \frac{\begin{bmatrix} k \\ t \end{bmatrix}_q}{q^{(n-k)(\delta-t-1)}},$$

where $\begin{bmatrix} a \\ b \end{bmatrix}_q = \prod_{i=0}^{b-1} \frac{q^{a-i}-1}{q^{b-i}-1}$ *is the q-ary Gaussian coefficient.*

Proof First, we observe that to present a lower bound on $L(\tau, n, k, \delta, q)$ $(L_I(t, n, k, \delta, q))$ it is sufficient to consider the list size for a given received subspace, i.e. an existence of one such received subspace with a given list size provides the desired lower bound. We consider a received word $\mathcal{R}$ of the same dimension k. Let $\mathcal{R} := \mathrm{rs}[\ I_k\ A_1\ ]$ for some $A_1 \in \mathbb{F}_q^{k\times(n-k)}$. Then

$$d_S(\mathcal{R}, \mathrm{rs}[\ I_k\ A\ ]) = 2d_R(A_1, A),$$

for any $A \in \mathbb{F}_q^{k\times(n-k)}$ (see e.g. [25]), and hence the distance between $\mathcal{R}$ and any codeword – and more generally any element from $\mathcal{G}_q(k, n)$ – is an even number. Thus, if τ is even, then $B^k_{\tau+1}(\mathcal{R}) = B^k_\tau(\mathcal{R})$ and hence $L_S(\tau+1, n, k, \delta, q) = L_S(\tau, n, k, \delta, q)$. Furthermore, if τ is even, $\mathrm{rs}[\ I_k\ A\ ]$ is in the ball around $\mathcal{R}$ of subspace radius τ if and only if A is in the ball around A_1 of rank radius $\tau/2$. It follows that the lower bound of the list size of classical Gabidulin codes for rank radius $\lfloor \tau/2 \rfloor$ is also a lower bound for the list size of lifted Gabidulin codes for subspace radius τ.

For the injection distance it holds that

$$d_I(\mathcal{R}, \mathrm{rs}[\ I_k\ A\ ]) = d_R(A_1, A)$$

and if follows right away that the lower bound of the list size of classical Gabidulin codes for rank radius t is also a lower bound for the list size of lifted Gabidulin codes for injection radius t.

The formula for the list size of classical Gabidulin codes can be found in [34]. □

For the rest of this section let $\tau = 2t$, then the two bounds of Theorem 37 are equal and asymptotically become:

$$\frac{\begin{bmatrix} k \\ t \end{bmatrix}_q}{q^{(n-k)(\delta-t-1)}} \sim q^{t(k-t)-(n-k)(\delta-t-1)} = q^{-t^2+nt-(n-k)(\delta-1)}. \tag{3}$$

(For $t = \delta - 1$ this bound becomes $q^{(\delta-1)(k-\delta+1)}$ which does not depend on n.) Similarly to [34], one can find the smallest value of radius t, when the exponent $-t^2 + nt - (n-k)(\delta-1)$ appearing in (3) becomes positive. When this is the case the list variety has a positive dimension and the size of the list grows polynomially with the field size. The following corollary shows that as a function of n the list size grows exponentially.

Corollary 38 *For any $0 \leq \epsilon < 1$ the list sizes $L_S(2t, n, k, \delta, q)$ and $L_I(t, n, k, \delta, q)$ are exponential in n if*

$$t \geq (n - \sqrt{n(n - 4\delta + 4\epsilon) + 4k\delta + 4k})/2.$$

6 Conclusion and Open Problems

The balls in $\mathcal{G}_q(k, n)$ with a center that is not necessarily in $\mathcal{G}_q(k, n)$ are considered with respect to two different distances: the subspace distance and the injection distance. Two different techniques are used for describing these balls: one is the Plücker embedding of $\mathcal{G}_q(k, n)$ and the second one is a rational parametrization of the matrix representation of the elements in $\mathcal{G}_q(k, n)$. These results can be used for list decoding of constant dimension codes. In particular, we investigate lifted Gabidulin codes and show that these can be described by linear equations in either the matrix representation or a subset of the Plücker coordinates. The union of these linear equations and the linear and bilinear equations which arise from the description of the ball of a given radius in the Grassmannian describe the list of codewords with distance less than or equal to the given radius from the received word. In contrast to the algorithms presented in [11,19] the algorithms presented in this paper work for the complete lifted Gabidulin codes for any set of parameters q, n, k, δ.

In fact, the theory of Section 4 holds for any linear rank-metric code, not only Gabidulin codes, hence also the algorithms from Section 5 work for any lifted linear rank-metric code.

One can easily extend the algorithms presented in this paper for unions of lifted Gabidulin codes of different length (cf. e.g. [26,31]). To do so, one needs to add a preliminary step in the algorithm where a rank argument decides, which of these lifted Gabidulin codes can possibly have codewords that are in the ball around the received word.

The storage needed for both our algorithms 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 want to improve this complexity by trying to decrease the size of the system of equations to solve in the last step of Algorithm 1 on one hand, or to find a better way to solve the system of bilinear equations in Algorithm 2 on the other. 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.

Acknowledgment

The authors wish to thank Antonia Wachter-Zeh for many helpful discussions. They also thank the anonymous reviewers for their valuable comments and suggestions that helped to improve the presentation of the paper.

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. Courtois, N. and Klimov, A. and Patarin, J. and Shamir, A., *Efficient algorithms for solving overdefined systems of multivariate polynomial equations*, Advances in cryptology—EUROCRYPT 2000 (Bruges), Lecture Notes in Comput. Sci. (1807), 392–407, Springer, 2000.
3. P. Delsarte, *Bilinear forms over a finite field, with applications to coding theory*, J. Combin. Theory Ser. A **25** (1978), no. 3, 226–241.
4. 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.
5. T. Etzion and N. Silberstein, *Codes and Designs Related to Lifted MRD Codes*, IEEE Trans. Inform. Theory, vol. 59, no.2, pp. 1004–1017, February 2013.
6. T. Etzion and A. Vardy, *Error-correcting codes in projective space*, IEEE Trans. Inform. Theory, vol. 57, no. 2, pp. 1165–1173, February 2011.
7. È. M. Gabidulin, *Theory of codes with maximum rank distance*, Problemy Peredachi Informatsii **21** (1985), no. 1, 3–16.

8. 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.
9. 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), pp. 183–189, January 2012.
10. V. Guruswami and C. Wang, *Explicit rank-metric codes list-decodable with optimal redundancy*, arXiv:1311.7084 [**cs.IT**], 2013.
11. 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).
12. W. V. D. Hodge and D. Pedoe, *Methods of algebraic geometry, vol. ii*, vol. 2, Cambridge University Press, 1952.
13. A. Kipnis, A. Shamir, *Cryptanalysis of the HFE Public Key Cryptosystem*, Advances in cryptology—CRYPTO '99 (Santa Barbara, CA), Lecture Notes in Comput. Sci. (1666), Springer, pp. 19–30, 1999.
14. S. L. Kleiman and D. Laksov, *Schubert calculus*, Amer. Math. Monthly **79** (1972), pp. 1061–1082.
15. 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.
16. 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.
17. 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.
18. H. Mahdavifar and A. Vardy. *Algebraic list-decoding on the operator channel*, in Proceedings of the IEEE International Symposium on Information Theory (ISIT), pp. 1193–1197, 2010.
19. H. Mahdavifar and A. Vardy. *List-decoding of subspace codes and rank-metric codes up to Singleton bound*, in Proceedings of the IEEE International Symposium on Information Theory (ISIT), pp. 1483–1492, 2012.
20. C. Procesi, *A primer of invariant theory*, Brandeis lecture notes, Brandeis University, 1982, Notes by G. Boffi.
21. J. Rosenthal and A.-L. Trautmann, *Decoding of subspace codes, a problem of schubert calculus over finite fields*, Mathematical System Theory - Festschrift in Honor of Uwe Helmke on the Occasion of his Sixtieth Birthday, CreateSpace, 2012.
22. 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.
23. N. Silberstein and T. Etzion, *Enumerative coding for Grassmannian space*, Information Theory, IEEE Transactions on **57** (2011), no. 1, 365–374.
24. N. Silberstein and T. Etzion, *Large constant dimension codes and lexicodes*, Advances in Mathematics of Communications, vol. 5, no. 2, pp. 177–189, 2011.
25. 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.
26. V. Skachek, *Recursive code construction for random networks*, IEEE Trans. Inform. Theory, vol. 56, no. 3, pp. 1378–1382, March 2010.
27. E. Thomae and C. Wolf, *Solving Systems of Multivariate Quadratic Equations over Finite Fields or: From Relinearization to MutantXL*, Cryptology ePrint Archive, Report 2010/596, 2010, eprint.iacr.org/.
28. A.-L. Trautmann, F. Manganiello, M. Braun, and J. Rosenthal, *Cyclic orbit codes*, IEEE Transactions on Information Theory, vol. 59, no. 11, pp. 7386–7404, 2013.
29. 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.
30. A.-L. Trautmann, N. Silberstein, and J. Rosenthal, *List Decoding of Lifted Gabidulin Codes via the Plücker Embedding*, Preproceedings of the International Workshop on Coding and Cryptography (WCC), Bergen, Norway, 2013, pp. 539–549.
31. A.-L. Trautmann, *Constructions, Decoding and Automorphisms of Subspace Codes*, PhD thesis, University of Zurich, Switzerland, 2013.
32. 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.
33. 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.
34. A. Wachter-Zeh, *Bounds on list decoding Gabidulin codes*, IEEE Transactions on Information Theory, pp. 7268-7277, 2013.
35. A. Wachter-Zeh and A. Zeh, *Interpolation-based decoding of interleaved Gabidulin codes*, Preproceedings of the International Workshop on Coding and Cryptography (WCC), Bergen, Norway, 2013, pp. 528–538.

Author/s:
Rosenthal, J; Silberstein, N; Trautmann, AL

Title:
On the geometry of balls in the Grassmannian and list decoding of lifted Gabidulin codes

Date:
2014-01-01

Citation:
Rosenthal, J., Silberstein, N. & Trautmann, A. L. (2014). On the geometry of balls in the Grassmannian and list decoding of lifted Gabidulin codes. Designs, Codes, and Cryptography, 73 (2), pp.393-416. https://doi.org/10.1007/s10623-014-9932-x.