21st International Symposium on
Mathematical Theory of Networks and Systems
July 7-11, 2014. Groningen, The Netherlands

Limitations of Polynomial-size List-decoding of Projective Space Codes

Kyle Marshall and Joachim Rosenthal

May 11, 2014

1 Introduction

Codes defined as sets of subspaces have received an increasing amount of attention since Kötter and Kschischang showed that they are suitable for correcting transmission errors in a network setting [6]. These codes are often called *subspace codes*. We will often view these codes as subsets of the Grassmann variety, and therefore we will refer to them as *projective space codes*. Much work has been done in creating families of projective space codes with good parameters and efficient decoding algorithms [8]. Recently, attention has also been focused on list-decoding of projective space codes [3, 10, 7]. It is this latter question that we examine more closely. In particular, we investigate how the geometry of a projective space code plays a role in the list-decoding problem.

2 Background

2.1 The List-Decoding Problem

Fix a finite field, $\mathbb{F}_q$, of q elements and an integer n. The projective geometry of $\mathbb{F}_q^n$, denoted $\mathrm{PG}(\mathbb{F}_q^n)$ is the set of all subspaces of $\mathbb{F}_q^n$. Equivalently, this is the set of all linear spaces of the projective space $\mathbb{P}^{n-1}(\mathbb{F}_q) := (\mathbb{F}_q^n \setminus \{0\})/\sim$, where $u \sim v$ if there exists $\alpha \in \mathbb{F}_q$ such that $u = \alpha v$.

Given two subspaces $\mathcal{U} \neq \mathcal{V} \subset \mathbb{F}_q^n$ we can define a metric on $\mathrm{PG}(\mathbb{F}_q^n)$ by

$$d_{\mathrm{S}}(\mathcal{U}, \mathcal{V}) = \dim(\mathcal{U} + \mathcal{V}) - \dim(\mathcal{U} \cap \mathcal{V}), \tag{1}$$

called the *subspace distance*. If $\mathcal{C} \subset \mathrm{PG}(\mathbb{F}_q^n)$ is such that for every $\mathcal{U}, \mathcal{V} \in \mathcal{C}$, $d_{\mathrm{S}}(\mathcal{U}, \mathcal{V}) \geq \delta$, then we say that $\mathcal{C}$ is a code of minimum distance at least δ. If δ is minimal, then we say that δ is the minimum distance of $\mathcal{C}$. A code of minimum distance δ is capable of uniquely correcting $\lfloor (1/2)(\delta - 1) \rfloor$ errors (with respect to d_{S}). The minimum distance of $\mathcal{C}$ is denoted by $d_{\mathrm{S}}^{\min}(\mathcal{C})$.

For the rest of this paper we consider only projective space codes whose elements all have the same dimension. For some fixed $k \leq n$, these codes belong to the (k, n)-*Grassmannian*, the set

ISBN: 978-90-367-6321-9

of subspaces of $\mathbb{F}_q^n$ of dimension k which we denote by $\mathrm{Gr}(k, \mathbb{F}_q^n)$. Such codes are called *constant-dimension codes*. We will also restrict our attention to received words $R \in \mathrm{Gr}(k, \mathbb{F}_q^n)$ although conceivably R could be a space of any dimension smaller than n.

One of the highlights of list-decoding for linear codes in the classical case was the construction of a polynomial time algorithm for list-decoding folded Reed-Solomon codes up to the Shannon limit [4]. Some attempts to list-decode projective space codes were undertaken in [7], however a polynomial time algorithm for list-decoding high rate codes remains elusive.

Definition 2.1. *Let $\mathcal{C} \subset \mathrm{PG}(\mathbb{F}_q^n)$ and fix $0 \leq t \leq 2k$. For a fixed subspace $R \in \mathrm{PG}(\mathbb{F}_q^n)$, define the $(t, \mathcal{C})$-list around R to be*

$$\mathcal{L}_{t,\mathcal{C}}(R) = \mathcal{C} \cap \mathcal{B}_t(R), \tag{2}$$

where $\mathcal{B}_t(R)$ is the ball of radius t.

If $t \leq \lfloor (1/2)(d_{\min}(\mathcal{C}) - 1) \rfloor$, then $|\mathcal{L}_{t,\mathcal{C}}(\mathcal{R})| \leq 1$ and producing this list is the unique decoding problem. Let $0 \leq \rho \leq 1$ and $L \geq 1$. A code $\mathcal{C} \subset \mathrm{Gr}(k, \mathbb{F}_q^n)$ is (ρ, L)-list-decodable if for any $R \in \mathrm{Gr}(k, \mathbb{F}_q^n)$, $|\mathcal{L}_{2k\rho,\mathcal{C}}(R)| \leq L$.

2.2 Lifted Rank-Metric Codes

One of the most ubiquitous families of constant dimension codes are the *lifted rank-metric* (LRM) codes. These codes are constructed by embedding a family of rank-metric codes into the Grassmanian in a particular way. LRM codes contain asymptotically optimal families of codes, and are the basis for the construction of other codes [2]. We consider lifting only from rank-metric codes which are linear.

Let $\mathcal{V} \subset \mathbb{F}_{q^{n-k}}^k$ be a subspace of dimension ℓ. We can represent every element $\alpha \in \mathbb{F}_{q^{n-k}}^k$ as a matrix $\overline{\alpha} \in \mathbb{F}_q^{k \times (n-k)}$ in the natural way. For $\alpha, \beta \in \mathbb{F}_{q^{n-k}}^k$, we can define the *rank distance* between α and β by $d_{\mathrm{R}}(\alpha, \beta) = \mathrm{rk}(\overline{\alpha} - \overline{\beta})$. The minimum rank distance is bounded above by $k - \ell + 1$. If this is attained, we say the code has *maximum rank distance* (MRD). Gabidulin codes are a particular construction using linearized polynomial evaluation [3] and are up to isomorphism the only known MRD codes. Gabidulin codes are an analog of Reed-Solomon codes in the classical case.

Definition 2.2. *The lifted rank metric (LRM) code of $\mathcal{V} \subset \mathbb{F}_{q^{n-k}}$ is given by*

$$C_{\mathcal{V}} = \{\mathrm{rowsp}[I_k \mid \overline{V}] \mid V \in \mathcal{V}\}.$$

The minimum subspace distance is given by $k + d_{\mathrm{R}}^{\min}(\mathcal{V})$.

Wachter studied [10] the list-decoding of rank-metric codes and showed for instance, that for Gabidulin codes there can be no polynomial time list-decoding algorithm when the radius of the decoding is larger than the Johnson bound. In the classical case for Reed-Solomon codes, this remains an open question. Ding in [1] shows that with high probability, a random rank-metric code of rate R can be list-decoded up to a $1 - R - \epsilon$ fraction of errors with list size $L \leq O(1/\epsilon)$.

3 The Role of Schubert Varieties

The Plücker embedding gives a map from $\mathrm{Gr}(k, \mathbb{F}_q^n)$ to $\mathbb{P}^{N-1}$, where $N = \binom{n}{k}$. The image is a variety cut out by quadratic equations called the *shuffle relations*. Trautmann et al. showed [9] that balls in the Grassmanian correspond to Schubert varieties in $\mathbb{P}^{N-1}$. Since Schubert varieties are given by linear equations (together with the shuffle relations), it is suggested that these equations can be used to develop list-decoding algorithm.

A Schubert variety can be described with respect to a complete flag. Schubert varieties have a rich structure, and a calculus for computing intersections of Schubert varieties is developed largely for $\mathbb{C}$ or $\mathbb{R}$ although not very extensively over finite fields [5]. We explore further the connection between list-decoding and Schubert varieties, and show that list-decoding amounts to interecting our code with a Schubert variety of certain type.

When $\mathcal{C}_\mathcal{V}$ is a lifted rank code from a linear space $\mathcal{V}$, $\mathcal{C}_\mathcal{V}$ can be defined by linear equations in the Plücker coordinates (together with the shuffle relations). Therefore, intersecting $\mathcal{C}_\mathcal{V}$ with a ball of some radius amounts to solving a system of linear and quadratic equations. While these equations are far too many to deal with practically, we explore how these equations can be simplified.

4 Bounds for List-decoding LRM Codes

Let $\mathcal{C}_\mathcal{V}$ be a LRM code from a linear MRD code $\mathcal{V}$ of dimension 1. It is clear that if $\rho < 1/2$, this corresponds to unique decoding and therefore $L = 1$ is the best possible bound. When $\rho \geq 1/2$, we can obtain the following lower bound for L.

Proposition 4.1. *Let $\mathcal{C}_\mathcal{V}$ be a lifted rank metric code from $\mathcal{V}$, a linear MRD code of dimension 1. If $\rho \geq 1/2$, we have*

$$L \geq q^{\left(\frac{\rho}{1-\rho}\right)}.$$

An open question is to find an non-trivial upper bound for L. The same problem exists in the case of list-decoding Gabidulin codes. In fact, we can view the problem of list-decoding Gabidulin codes as a special case of the list-decoding problem for LRM codes.

Proposition 4.2. *Let $\mathcal{V}$ a Gabidulin code of dimension 1. If $R \in \mathrm{Mat}_{k\times(n-k)}(\mathbb{F}_q)$ and $0 \leq \rho < 1$, then*

$$|\mathcal{B}_{k\rho}(R) \cap \mathcal{V}| = |\mathcal{B}_{2k\rho}(\mathrm{rowsp}[I_k|R] \cap \mathcal{C}_\mathcal{V})|.$$

Unlike Gabidulin codes for which the question regarding the size of lists up to the Shannon limit remains open, Lifted Gabidulin codes can never have polynomial list size as soon as the list-decoding radius exceeds unique decoding. In this talk we show how the geometry of the Grassmann plays an interesting role in helping to determine the size of the list. In particular, we examine how the structure of the received space can help us predict the size of our lists.

References

[1] Yang Ding. On list-decodability of random rank metric codes. *CoRR*, abs/1401.2693, 2014.

[2] Tuvi Etzion and Alexander Vardy. Error-correcting codes in projective space. *IEEE Transactions on Information Theory*, 57(2):1165–1173, 2011.

[3] Maximilien Gadouleau and Zhiyuan Yan. Constant-rank codes and their connection to constant-dimension codes. *IEEE Trans. Inf. Theor.*, 56(7):3207–3216, July 2010.

[4] Venkatesan Guruswami and Atri Rudra. Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy. *CoRR*, abs/cs/0511072, 2005.

[5] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[6] Ralf Koetter and Frank R. Kschischang. Coding for errors and erasures in random network coding. *CoRR*, abs/cs/0703061, 2007.

[7] Hessam Mahdavifar and Alexander Vardy. Algebraic list-decoding of subspace codes. *CoRR*, abs/1202.0338, 2012.

[8] Anna-Lena Trautmann, Felice Manganiello, Michael Braun, and Joachim Rosenthal. Cyclic orbit codes. *CoRR*, abs/1112.1238, 2011.

[9] Anna-Lena Trautmann, Natalia Silberstein, and Joachim Rosenthal. List decoding of lifted gabidulin codes via the plücker embedding. *CoRR*, abs/1301.2165, 2013.

[10] Antonia Wachter-Zeh. Bounds on list decoding of rank-metric codes. *IEEE Transactions on Information Theory*, 59(11):7268–7277, 2013.