Subspace Codes for Random Network Coding

1 Classical Coding Theory

At its most basic, algebraic coding theory studies the balance between adding mathematical redundancy to data versus the cost of sending the redundancy. The basic problem to be solved is that there is a sender trying to send data through a noisy channel to a receiver, but the noise may cause errors to occur during the transmission. Thus to fix this problem we encode the data into a codeword, typically a vector over a finite alphabet, and send the codeword across the channel. Thus, if the received word does not exactly match any of the expected codewords, it is decoded to the closest (by some appropriate metric on the vectors) codeword. This way we can detect and correct errors in transmission. However, to accomplish this task, we must have large collections of vectors which are far apart by an appropriate distance. Additionally, we need to be able to efficiently decode the received word to the closest codeword.

2 Random Network Coding Theory

In random network coding, we have a network, that is a directed graph with sources and sinks, across which we want to send data. As the data moves through the network it is collected at nodes, which compile the incoming data and send it on as a linear combination. Thus the only information that needs to be maintained across the network is the linear combinations of the data. However, this causes errors and erasures to propagate greatly, since each linear combination after the error or erasure continues to be corrupted. In order to correct these issues Kötter and Kschischang [7] introduced an algebraic approach for error correcting in random network coding, by using subspaces themselves as the codewords rather than vectors. Using subspaces makes sense, since a subspace is exactly the object which stores linear combinations, the data sent through the network. Additionally, subspace codes are the q-analog of packing designs, so they have also been studied from a combinatorial perspective and some of these codes have be constructed as packing designs, see [1].

3 Introduction to Subspace Codes

Let $\mathbb{F}_q$ be a finite field of size q. Let $\mathbb{F}_q^n$ be the space of row vectors with entries in $\mathbb{F}_q$. Define the subspace distance as

$$\mathrm{d}_S(\mathcal{U},\mathcal{V}) := \dim(\mathcal{U}) + \dim(\mathcal{V}) - 2\dim(\mathcal{U}\cap\mathcal{V}).$$

Importantly, the subspace distance is a metric and $\mathrm{d}_S(\mathcal{U},\mathcal{V}) = 0$ if and only if $\mathcal{U} = \mathcal{V}$, which shows us why we subtract twice the dimension of the intersection. The idea of the subspace distance is that two subspaces are close together if they share many of the same linear combinations, which makes sense with our goals.

We say that a nonempty collection, $\mathcal{C}$, of subspaces of $\mathbb{F}_q^n$ is a $(n, N, d)_q$ *subspace code*, if $N = |\mathcal{C}|$ and $\mathrm{d}_S(\mathcal{U},\mathcal{V}) \geq d$ for all $\mathcal{U},\mathcal{V} \in \mathcal{C}$. In this case, we denote the subspace distance of a code by, $\mathrm{d}_S(\mathcal{C}) = d$. Many times we restrict ourselves to the Grassmannian, that is, the set of k dimensional subspace of $\mathbb{F}_q^n$, which we denote $\mathcal{G}_q(n,k)$. If $\mathcal{C} \subset \mathcal{G}_q(n,k)$ then we say that $\mathcal{C}$ is a $(n, N, d, k)_q$ *constant dimension subspace code*. If $\mathcal{C}$ is of constant dimension k then $\mathrm{d}_S(\mathcal{U},\mathcal{V}) = 2(k-\dim(\mathcal{U}\cap\mathcal{V}))$, for all $\mathcal{U},\mathcal{V} \in \mathcal{C}$. Thus the distance is even for a constant dimension code. We should note that $0 < \mathrm{d}_S(\mathcal{C}) \leq 2k$, and $\mathrm{d}_S(\mathcal{C}) = 2k$ only if all of the codewords intersect trivially.

A constant dimension code, $\mathcal{C}$, with distance $2k$ is called a *partial spread code*. A partial spread code for which every 1 dimensional subspace is contained in exactly one subspace of the code, is called a *spread code*. Spread codes, are the q-analogues of combinatorial spreads and have been well studied in this context. It is well known that spread codes only occur in the case where $k|n$

and have cardinality $\frac{q^n-1}{q^k-1}$. Spread codes are optimal since they achieve the Singleton bound and can be efficiently decoded, see [2].

Another major class of subspace codes are derived from a type of matrix codes called rank metric codes. We define the *rank metric* for two matrices $X, Y \in \mathbb{F}_q^{m\times n}$ as

$$\mathrm{d}_R(X,Y) := \mathrm{rank}\,(X-Y).$$

Like the subspace distance, the rank distance is also a metric and it is easy to see that $\mathrm{d}_R(X,Y) = 0$ if and only if $X = Y$. A *linear rank metric code* is a subspace $\mathcal{C} \subset \mathbb{F}_q^{m\times n}$ endowed with the rank metric. There are many ways to utilize these matrix codes for subspace codes, but the easiest way is to lift the matrices to subspaces. We define the lifting of a matrix $X \in \mathbb{F}_q^{k\times n}$ as $\Lambda(X) = \mathrm{rowspace}\,(I_{k\times k}\ X)$. Notice that $\dim \Lambda(X) = k$ for all X, so we can construct a constant dimension subspace code $\mathcal{C} := \{\Lambda(X) \mid X \in \mathcal{C}_R\}$ from any rank metric code $\mathcal{C}_R$. It is straight forward to show that for a lifted rank metric code $\mathrm{d}_S(\mathcal{C}) = 2\mathrm{d}_R(\mathcal{C}_R)$. This construction was originated by Kötter and Kschischang in [7] and has been expanded upon by Etzion and Silberstein in [3] as well as others.

There are other known constructions and my research focuses on looking at new constructions as well as refining some currently known constructions.

4 Cyclic Orbit Codes

One of the main constructions I have studied is that of irreducible cyclic orbit codes, which were introduced by Rosenthal and Trautmann in 2013, [8]. Cyclic subspace codes are subspace codes which are closed under the cyclic shift operation, and were introduced by Etzion and Vardy in [4], but were also constructed by Kohnert and Kurz in [6]. They are very large codes and it can be shown that they are unions of irreducible cyclic orbit codes. In order to gain more knowledge of these cyclic subspace codes, I looked into a way to find the cardinality and distance of irreducible cyclic orbit codes, the building blocks of cyclic subspace codes.

For this section of this statement, we will utilize an $\mathbb{F}_q$-linear isomorphism between $\mathbb{F}_q^n$ and $\mathbb{F}_{q^n}$. This means we will think that a subspace $\mathcal{U}$ is a subspace of $\mathbb{F}_{q^n}$, considerd as a vector space over $\mathbb{F}_q$.

Definition 1. Fix a primitive element $\alpha \in \mathbb{F}_{q^n}$, that is, an element which is a generator of the multiplicative group of the field, $\mathbb{F}_{q^n}^*$. Let $\mathcal{U}$ be a k-dimensional subspace of $\mathbb{F}_{q^n}$. The *(primitive) cyclic orbit code* generated by $\mathcal{U}$ is defined as the set

$$\mathrm{Orb}(\mathcal{U}) := \{\mathcal{U}\alpha^i \mid i = 0, 1, \ldots, q^n - 1\},$$

where $\mathcal{U}\alpha^i := \{u\alpha^i \mid u \in \mathcal{U}\}$.

Note that $u\alpha^i$ is the standard multiplication in the field $\mathbb{F}_{q^n}$. Furthermore, since $\dim\left(\mathcal{U}\alpha^i\right) = \dim(\mathcal{U})$, the code $\mathrm{Orb}(\mathcal{U})$ is a constant dimension code. We will assume that $\mathrm{Orb}(\mathcal{U}) \subset \mathcal{G}_q(n,k)$ for the rest of this section.

If we consider the subfield $\mathbb{F}_{q^k}$ as a $\mathbb{F}_q$ vector space of $\mathbb{F}_{q^n}$, then we can show that $\mathrm{Orb}(\mathbb{F}_{q^k})$ is a spread code. This fact shows that cyclic orbit codes are a natural generalization of spread codes. In my research, I wanted to find properties of a subspace $\mathcal{U}$, which would contribute to cardinality and distance of the code $\mathrm{Orb}(\mathcal{U})$. Since $\mathbb{F}_{q^k}$ generates a spread code, I investigated how the other subfields of $\mathbb{F}_{q^n}$ relate to the cardinality and distance of $\mathrm{Orb}(\mathcal{U})$. Recall, that any subfield of $\mathbb{F}_{q^n}$ is of the form $\mathbb{F}_{q^r}$, where $r|n$. To continue we will need the idea of friends of a subspace.

Definition 2. Let $\mathcal{U}$ be a subspace of $\mathbb{F}_{q^n}$. A subfield $\mathbb{F}_{q^r}$ of $\mathbb{F}_{q^n}$ is called a *friend* of $\mathcal{U}$ is $\mathcal{U}$ is a vector space over $\mathbb{F}_{q^r}$ with scalar multiplication being the multiplication in the field $\mathbb{F}_{q^n}$. The largest friend (with respect to cardinality) is called the *best friend* of $\mathcal{U}$.

Knowing the best friend of a subspace, $\mathcal{U}$, immediately tells us the cardinality of the code $\mathrm{Orb}(\mathcal{U})$ as well as some information about the distance of the code.

Proposition 3. *Let $\mathbb{F}_{q^r}$ be the best friend of $\mathcal{U}$. Then*

$$|\mathrm{Orb}(\mathcal{U})| = \frac{q^n-1}{q^r-1} \qquad \textit{and} \qquad 2r \leq \mathrm{d}_S(\mathrm{Orb}(\mathcal{U})) =\leq 2k.$$

A proof of this proposition can be found in [5]. In fact, we can get better results about the distance of an cyclic orbit code. It turns out that $\mathrm{d}_S(\mathrm{Orb}(\mathcal{U})) = 2(k-sr)$, where s is the maximum dimension of $\mathcal{U} \cap \mathcal{U}\alpha^i$ as a vector space over the best friend $\mathbb{F}_{q^r}$, for $i = 1, \ldots, \frac{q^n-1}{q^r-1}$. We have proved a construction of $\mathcal{U}$ that gives a cyclic orbit code of minimum possible distance $2r$, and have other conditions on $\mathcal{U}$ that give poor distance. This helps aviod poor choices for $\mathcal{U}$. Additionally, we refine a result from [8], which utilizes multisets, as well as the best friend, to compute the distance of these codes.

5 A Linkage Construction

As mentioned in section 2, there are many types of constructions for subspace codes. However, each of these constructions requires an entirely new code to be build for each set of parameters. For many of these constructions this is a difficult process that is done in large part by careful computer search. The following construction is a recursive construction, which links two different subspace codes to create a larger (in terms of cardinality) and longer (in terns of n) subspace code. This is useful because, once shorter codes have been developed, we can quickly and easily create longer codes.

Theorem 4. *For $i = 1, 2$ let $\mathcal{C}_i = \{\mathrm{rowspace}\, U_{i,l} \mid l \in [N_i]\}$ be a $(n_i, N_i, d_i, k)_q$-code. Thus $U_{i,l}$ are matrices of rank k in $\mathbb{F}_q^{k\times n_i}$ for all i, l. Let $\mathcal{C}_R$ be a $k \times n_2$ linear rank metric code, such that $|\mathcal{C}_R| := N_R$ with rank distance $\mathrm{d}_R(\mathcal{C}_R) = d_R$. Define the subspace code $\widetilde{\mathcal{C}}$ of length $n := n_1 + n_2$ as $\widetilde{\mathcal{C}} = \widetilde{\mathcal{C}}_1 \cup \widetilde{\mathcal{C}}_2 \cup \widetilde{\mathcal{C}}_3$, where*

$$\begin{aligned}
\widetilde{\mathcal{C}}_1 &= \{\mathrm{rowspace}\ (U_{1,l}, 0_{k\times n_2}) \mid l \in [N_1]\},\\
\widetilde{\mathcal{C}}_2 &= \{\mathrm{rowspace}\ (0_{k\times n_1}, U_{2,l},) \mid l \in [N_2]\},\\
\widetilde{\mathcal{C}}_3 &= \{\mathrm{rowspace}\ (U_{1,l}, M) \mid l \in [N_1], M \in \mathcal{C}_R \backslash \{0\}\}.
\end{aligned}$$

Then $\widetilde{\mathcal{C}}$ is a $(n, N, d, k)_q$ code, where $N = N_2 + N_1 N_R$ and $d = \min\{d_1, d_2, 2d_R\}$.

While this construction, which I will refer to as the linkage construction, does not exceed any known lower bounds for cardinality, it comes close to many of these bounds and beats many codes. Additionally, the linkage construction gives a systematic and recursive approach to finding large codes, which is a selling point because all the codes which beat the linkage construction rely heavily on computer search to generate the code for each set of parameters. I am currently looking into an efficient decoding algorithm for the linkage construction and in the case where we assume $\mathcal{C}_R$ is also a subspace code, we have an efficient decoding algorithm, as long as the underlying codes have an efficient decoding algorithm.

This construction works particularly nicely in a special case which uses partial spread codes. However, to do this, we must refine the linkage construction to a special case. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be

partial spreads of maximum cardinality, $V \in \mathbb{F}_q^{k\times n_2}$ be a full rank matrix, $M \in \mathrm{GL}_{n_2}(\mathbb{F}_q)$ be the companion matrix of a primitive polynomial of degree n_2, and $\mathcal{C}_R = \{VM^i \mid 0 \leq i \leq q^n - 2\}$ in theorem 4. The resulting code $\widetilde{\mathcal{C}}$ is then a partial spread code. Although it is still an open problem to find the maximum cardinality of a partial spread in most cases, it is know in the case $q = 2$, $k = 3$. For this case, we have shown that the refined linkage construction gives another construction for maximum partial spreads over $\mathbb{F}_2$ with dimension 3, for all n. A preliminary form of the linkage construction which utilizes the ideas of primitive cyclic orbit codes can be found in [5].

6 Undergraduate Research

As an undergraduate I was able to participate in two different undergraduate research projects, one of which was funded by the Center for Undergraduate Research in Mathematics. These opportunities shaped my mathematical career and have inspired me to do research with undergraduates. One of the reasons I research in coding theory is because it is easily accessible to undergraduates. Not only it is an active research area but also can easily be explained to people with just basic math skills. My research only requires basic knowledge of vector spaces, linear algebra and finite fields to get started, which enables many undergraduates to research in coding theory early on in their mathematical career. Since it has real world applications, but also can be viewed from a pure math standpoint, coding theory appeals to mathematicians of many different inclinations. I would love to work with students on new constructions of subspace codes or on optimizing known constructions. Working with constructions always requires the use of programming to compute examples of such codes, which is another way to give students a project which they can get started with quickly. I certainly see my research career being focused around undergraduate involvement.

References

[1] M. Braun and J. Reichelt. q-analogs of packing designs. *J. Combin. Des.*, 22(7):306–321, 2014.

[2] F. Manganiello E. Gorla and J. Rosenthal. An algebraic approach for decoding spread codes. *Adv. Math. Commun.*, 6(4):443–466, 2012.

[3] T. Etzion and N. Silberstein. Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams. *IEEE Trans. Inform. Theory*, 55(7):2909–2919, 2009.

[4] T. Etzion and A. Vardy. Error-correcting codes in projective space. *IEEE Trans. Inform. Theory*, 57(2):1165–1173, 2011.

[5] K. Morrison H. Gluesing-Luerssen and C. Troha. Cyclic orbit codes and stabilizer subfields. arXiv:1403.1218. To appear in *Advances in Mathematics of Communications.*

[6] A. Kohnert and S. Kurz. Construction of large constant dimension codes with a prescribed minimum distance. In *Mathematical methods in computer science*, volume 5393 of *Lecture Notes in Comput. Sci.*, pages 31–42. Springer, Berlin, 2008.

[7] R. Kötter and F.R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Trans. Inform. Theory*, 54(8):3579–3591, 2008.

[8] J. Rosenthal and A.-L. Trautmann. A complete characterization of irreducible cyclic orbit codes and their pl ucker embedding. *Designs Codes Cryptography*, 66:275–289, 2013.