A Summary of Previous Work

Ziquan Yang

August 22, 2014

1 Introduction

In order to correct errors efficiently, we hope to be able to reconstruct the information by accessing only a few other bits. As far as we concern, a linear code C is essentially a finite vector space, so in mathematical language, the above requirement amounts to requiring that for any coordinate, there exists a parity check of low weight in $C^{\perp}$ that contains the given coordinate in its support. Such codes are called *Locally Repairable Codes*. The set of all low weight parity checks used to cover the coordinates is called a *Repair Group*. Prof. Calderbank and his graduate student Sree have already done some work showing some interactions between repair groups, minimum distance and rate of the code. However, we want to understand something about the codes with more than one repair groups.
Cyclic codes are especially apt at constructing disjoint repair groups, a special case of our interest, so at the beginning of the research, Prof. Calderbank instructed me to fimilarize myself with some properties of cyclic codes.

2 Cyclic Codes

2.1 Fourier Transform

DFT is a map that maps a vector v of length n in base field $\mathbb{F}_p$ (time domain) to a vector V in $\mathbb{F}_{p^n}$ (frequency domain). Let α be a primitive root in $\mathbb{F}_{p^n}$, then

$$V_i = \sum_{j=0}^{n-1} \alpha^{ij} v_j$$

Of course, not all vectors in $\mathbb{F}_{p^n}$ could be the image of DFT. We know that a vector V is an image if and only if it satisfies the conjugacy constraint: $V_i = V_{pi}$. Clearly, if α^i is a zero to v, then we have $V_i = 0$. Some computation will show that convolution of two vectors in the time domain corresponds to the componentwise multiplication in the frequency domain: $w(x) \equiv u(x)v(x)(mod x^n - 1) \Leftrightarrow W_i = U_i V_i, \forall i$. A not so clear correspondence is that the hamming weight of v equals to *linear complexity* of V.

2.1.1 A Simple Application

Let $C = \{c = (c_i) \in F_2^{N-1} | \sum_{i=0}^{N-2} c_i \alpha^{ij} = 0, \forall j \not\equiv 0(mod 3)\}$. Let's count the number of codewords of weight 3 in C. Taking $N = 16$ as a example, we see that all codewords in frequency domain must look like:

$$100\Lambda_3 00\Lambda_3^2 00\Lambda_3^3 00\Lambda_3^4 00$$

Apply conjugacy constraint, then we have $\Lambda_3^5 = 1$. Conversely, all such Λ_3 gives a valid codeword. Thus we have 5 codewords of weight 3. It is easy to observe that the answer in the general case is simply $2^{N-1}/3$.

2.1.2 Linear Recurrence

The concept of linear recurrence in a finite field arises naturally in the above example and has been studied thoroughly. More details could be found in [5].

2.2 Minimum distance

Up to now there does not exist a general method to compute the minimum distance of a cyclic code given the defining set. Yet several theorems have been proposed to give a lower bound on the minimum distance by exploinnting *continuity* of zeros. The BCH bound, a simple-minded bound, says that $d-1$ consecutive zeros will give a minimum distance of at least d. Hartmann and Tzeng, Roos and John van Lint improved this bound by allowing occassional omissions in the continuous sequence of zeros. John van Lint proposed a *cyclic shift* argument that could be used to derive the other three bounds. However, though the *cyclic shift* argument sometimes performs better than the Roos Bound, John van Lint did not give a systematic method of determining the most effective use of the argument.

3 Weight Distribution

Since the repair groups essentially provide some information on the weight distribution of the dual code, it may be useful to know something about weight distribution and its relationship to rank.

3.1 Generalized Hamming Weights

Generalized Hamming Weight was first studied by Victor Wei.

Definition 3.1.

$$d_r(C) := \min\{|\mathrm{supp(D)}| \mid \mathrm{D} \subseteq \mathrm{C}, \mathrm{rank(D)} = \mathrm{r}\}$$

The two most important properties of generalized hamming weights are:

Theorem 3.2. (Monotinicity)
For an $[n,k]$ code C with $k > 0$, we have

$$1 \leq d_1(C) < d_2(C) < \cdots < d_k(C) \leq n$$

Theorem 3.3. (Duality)

$$\{d_r(C)|1 \leq r \leq k\} \bigcap \{n+1-d_r(C^\perp) \mid 1 \leq r \leq n-k\} = \varnothing$$

or equivalently

$$\{d_r(C)|1 \leq r \leq k\} \bigcup \{n+1-d_r(C^\perp) \mid 1 \leq r \leq n-k\} = [n]$$

The significance of Duality is that it is one bridge to connect the weight/rank information of a code to that of its dual. More information on generalized hamming weight can be found in [1]. Some applications to cyclic codes can be found in [2].

3.2 MacWilliams Identities

MacWilliams Identities give a thorough connection of weight distribution of a code to that of its dual. Once you know one you can compute the other. However, at this stage we do not know yet how to use this theorem to deduce something interesting based on the constraints we impose on the dual. The main difficulties is: we require the repair group to *cover* the coordinates, which does not readily translates to useful information about the weight distribution of the dual. As for MacWilliams Identities themselves, [4] is a good reference to related topics.

4 Bounds on Dimensions

This is essentially a summary of our current toolbox in the single repair group case. The first two showed up in Sree's paper, and the third one was suggested by Prof. Calderbank.

4.1 Punctured Code Argument

The idea of punctured code argument is to find a set of coordinates that does not contain the support of any codeword. Thus we have find a injection of a code to a punctured code of smaller dimension. An example of this argument can be found in the proof of Theorem 1 in Sree's paper.

4.2 $C^\perp$ Rank Argument

The idea of $C^\perp$ rank argument is simply to give a lower bound for the rank of $C^\perp$ based on the constraints we have put on it. An example of this argument can be found in Theorem 3 in Sree's paper.

4.3 Subcode Argument

The idea of subcode argument is to "kill off" codewords of certian weight by imposing a few more parity checks, thereby creating a subcode whose dimension is easier to bound. Then we know a bound of the original code since we have only killed a limited number of ranks. More information can be found in my report "Subcode Argument".

4.4 Coset Assignment

The question of assigning vectors from one vector space to different images in a smaller space with a linear transformation naturally comes up in the proof of Theorem 3 in Sree's paper. An injection of vectors in vector space to another can be extended successfully to a linear transformation, not necessarily in a unique way, between the two vector spaces as long as the injection respects the linear dependence relations among the vectors. I want to understand when such an injection is possible and when certain bounds we proved with coset assignment are achievable. More information can be found in my report "Linear Embedding".

5 Multiple Repair Groups

I have to admit that I have not yet made much progress towards interactions of two repair groups. Even before we impose the minimum distance, we do not know much about the optimal rank of a code if no addition constraints are imposed.

5.1 A Simple Construction

Theorem 5.1. *Let C be a cyclic code of length $2^m - 1$ with set of zeros A. Suppose $t_1, t_2 \mid 2^m - 1$. If $t_1, t_2 \nmid i$ for each $\alpha_i \in A$, where α is a primitive root, then for each coordinate k, there exist a codeword of weight t_1 and another with weight t_2 which have k in their supports.*

5.2 Bounds on Dimension Assuming Disjointness

We are able to deduce something about the rank of a code when we assume both repair groups are disjoint. Suppose we have a doubly repairable code C with localities $r_1 = 2$ and $r_2 = 4$ of length $15m$ for some $m \geq 1$ and suppose we have two disjoint repairable groups. Let $P_i \in C^\perp, 1 \leq i \leq 5m$ be parity checks of weight 3 and $Q_j \in C^\perp, 1 \leq j \leq 3m$ be parity checks of weight 5. Then we are able to show the following result:

$$7m \leq \text{rank}\{P_1, P_2, \cdots, P_{5m}, Q_1, Q_2, \cdots, Q_{3m}\} \leq 8m - 1$$

Moreover, every integer in the above bound is achieved by some codes. This is reassuring since when disjointness is assumed, it is still likely that our cyclic code construction gives an optimal code. However, even when we assume disjointness and optimality, there are still myriad possible arrangements of the two repair groups and we have not yet find an example of how to impose the minimum distance to a fixed one.

5.3 Failure in General Case

It might be appealing to make the hypothesis that the $7m$ bound in dimension holds in general, where we do not assume disjoint repair groups. However, this is not true and a concrete counterexample is contructed. Let $m = 8$, $n = 120$, we divide the coordinates into 15 blocks, each of which is of length 8. For each block, consider the following matrix:

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

We see that rank$M = 3$ and it covers all 8 coordinates with a parity check of weight 5 and 6 coordinates with a parity check of weight 3, leaving out two in the middle. There are $2 \times 15 = 30$ coordinates uncovered in total and we can cover them with 10 parity checks of weight 3. Together with $M \otimes I_{15}$, we have constructed a $C^\perp$ with two repairable groups with total rank

$$3 \times 15 + 10 = 55 < 56 = 120 \times \frac{7}{15}$$

From the counterexample we also see that the actual lower bound is contingent on m, which makes the general case even harder to handle.

6 Continuation

As Prof. Calderbank suggested, my plan in near future is to understand [3], which connects generalized hamming weight to the discussion of rank. Still, our main focus is on doubly repairable codes, though any other discoveries about LRC are also welcome. During the summer I begin to realize that there are interesting connections of finite geometry and

combinatorial design to codes. These topics are not included in this summary since I have not made much use of them yet. As for my normal coursework, I am taking *Groups, Rings, and Fields*, in which I am supposed to learn some Galois Theory. I will also do some reading in the neighborhood of what interests me and [4] is a comprehensive reference book to serve this purpose. I have also decided to take a research independent study with Prof. Calderbank so that I can dedicate more time to this project.

References

[1] V. K. Wei, "Generalized Hamming weights for linear codes", *IEEE Trans. Inform. Theory*, vol. 37, pp.1412-1418, Sept. 1991

[2] G. L. Feng, K. K. Tzeng and V.K. Wei, "On the Generalized Hamming Weights of Several Classes of Cyclic Codes", *IEEE Trans. Inform. Theory*, vol. 38, pp.1125-1130, Sept. 1992

[3] N. Prakash, V. Lalitha and P. Vijay Kumar, "Codes with Locality for Two Erasures", *2014 IEEE International Symposium on Information Theory*, pp. 1962-1966

[4] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge University Press, UK 2003.

[5] R. Lidl, H. Niederreiter, *Finite Fields (Encyclopedia of Mathematics and its Applications)*. Cambridge University Press, UK 2008.