Correcting Grain-Errors in Magnetic Media

Ryan Gabrys*, Eitan Yaakobi†, and Lara Dolecek*
*University of California, Los Angeles †California Institute of Technology
rgabrys@ucla.edu, dolecek@ee.ucla.edu yaakobi@caltech.edu

***Abstract*—This paper studies new bounds and constructions that are applicable to the combinatorial granular channel model previously introduced by Sharov and Roth. We derive new bounds on the maximum cardinality of a grain-error-correcting code and propose constructions of codes that correct grain-errors. We demonstrate that a permutation of the classical group codes (e.g., Constantin-Rao codes) can correct a single grain-error. In many cases of interest, our results improve upon the currently best known bounds and constructions. Some of the approaches adopted in the context of grain-errors may have application to other channel models.**

I. Introduction

Granular media is a promising magnetic recording technology that currently presents formidable challenges to achieving capacity. One of the main issues with granular media is the uncertainty of the locations of the grains in the underlying recording medium. Typically, this medium is organized into grains whose locations and sizes are random. Information is stored by controlling the magnetization of the individual grains so that each grain can store a single bit of data [18], [19].

The read and write processes are typically unaware of the locations of the grains. As a result, the medium is divided into evenly spaced bit cells and the information is written into these bit cells [10]. In the traditional setup, the bit cell is usually larger than a single-grain. When the size of the bit cells is reduced enough, the effects of the random positions of the grains become pronounced. In particular, in [19] a one-dimensional channel model was studied that illustrated the effects of having grains with randomly selected lengths of 1, 2, or 3 bits. When grains span more than a single bit cell, the polarity of a grain is set by the last bit written into it. The errors manifest themselves as overwrites (or ***smears***) where the last bit in the grain overwrites the preceding bit in the grain. In this work, the focus is on grains of length one or two bits. A ***grain-error*** is an error where the information from one bit overwrites the information stored in the preceding bit in the grain. Without loss of generality, and as in [10], our model assumes that the first bit smears the following adjacent bit in the grain.

In [15], Sharov and Roth presented combinatorial bounds and code constructions for granular media. In [7], Iyengar, Siegel, and Wolf studied a related model from an information-theoretic perspective. In [10], Mazumdar, Barg, and Kashyap introduced a channel model and studied coding methods for a one-dimensional granular magnetic medium. In [10], the focus was on binary alphabets and the types of errors studied in [10] will be referred in this work as ***non-overlapping grain-errors***. In [15], Sharov and Roth generalized the model and considered non-binary alphabets as well as ***overlapping grain-errors***. Overlapping grain-errors permit the occurrence of two errors in consecutive positions whereas non-overlapping grain-errors cannot be adjacent. Note that there is no distinction between a non-overlapping single grain-error and an overlapping single grain-error. In this work, we restrict our attention only to the overlapping grain-error model. We say that a code is a ***t-grain-error-correcting code*** if it can correct up to t overlapping grain-errors. In both [10] and [15], bounds and constructions were given. Recently, in [8] some of the techniques from [9] were adopted to obtain improved upper bounds on the maximum cardinalities of non-overlapping grain-error codes.

The main contribution of this paper is to construct codes that correct grain-errors. We show that the class of group codes from [2] is a special case of our general code construction. In addition, and similar to [8], we provide non-asymptotic upper bounds on the cardinalities of t-grain-error-correcting codes, with an explicit expression for the cases where $t = 1, 2, 3$. We show that in many cases our bounds and constructions improve upon the state of the art results from [10] and [15].

Section II formally defines the channel model and introduces the notation and tools used for the remainder of the paper. Section III improves upon the existing upper bounds from [15]. Section IV contains constructions for codes that correct grain-errors and a related type of error which we refer to as mineral-errors. Lower bounds on the cardinalities for some of these codes are then derived in Section V. Section VI revisits the general approach to correcting grain/mineral-errors from Section IV-B, and identifies additional codes for certain code lengths. Section VII concludes the paper. Preliminary results of this work are presented in [4].

II. Preliminaries

In this section, we describe in detail the structure of grain-errors. Afterwards, we introduce some key notation. Section II-A introduces the errors of interest. Section II-B reviews the tools which will be used for computing upper bounds. Section II-C briefly introduces some graph notation. Section II-D reviews some distance metrics and group codes that will be useful for constructing grain-error-correcting codes. Finally, Section II-E includes some Fourier analysis tools useful for computing lower bounds for grain-error codes.

A. Grain-errors and mineral-errors

In this subsection, we formally introduce the notation and the errors of interest that will be studied in this work. We consider the case where each grain contains either one or two bits of data. A grain-error causes the two bits in the same two-bit grain to either both be 0 or both be 1; the error operation can be interpreted as a ***smearing***. Following the setup of [10], we assume that the first bit smears the second. The problem of interest is how to correct grain-errors when the locations and lengths of the grains are unknown to both the encoder and decoder.

Before continuing, we provide a formal definition of a t-grain-error. For a vector $\boldsymbol{x} \in GF(2)^n$, $wt(\boldsymbol{x})$ refers to the Hamming weight of $\boldsymbol{x}$ and $supp(\boldsymbol{x})$ denotes the set of indices of $\boldsymbol{x}$ with non-zero values.

Definition 1. *Let $t \geq 1$ be an integer. Suppose a vector $\boldsymbol{x} \in GF(2)^n$ was stored. Let $\boldsymbol{e_x} = (e_1, \ldots, e_n) \in GF(2)^n$, and suppose the vector $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e_x}$ was read. Then, we say that $\boldsymbol{e_x}$ is a* ***t*-grain-error for** *$\boldsymbol{x}$ if the following holds:*

1) *$wt(\boldsymbol{e_x}) \leq t$ and $e_1 = 0$,*
2) *For $2 \leq i \leq n$, if $e_i \neq 0$, then $x_i \neq x_{i-1}$.*

Note that $\boldsymbol{e_x}$ depends on the input vector $\boldsymbol{x}$. For shorthand, we say that $\boldsymbol{e_x}$ is a t-grain-error if the vector $\boldsymbol{x}$ is clear from the context. Notice in Definition 1 that an error at position i where $2 \leq i \leq n$ can be interpreted as a smearing where the value of $\boldsymbol{x}$ at position $i-1$ smears the value of $\boldsymbol{x}$ in position i.

A code that can correct any t-grain-error will be referred to as a ***t-grain-error-correcting code***. For shorthand, a code that can correct a single grain-error will also be referred to as a ***single-grain code***. More generally, codes that correct a prescribed number of grain-errors are called ***grain codes***. The maximum size of a t-grain-error-correcting-code of length n will be referred to as $M(n,t)$.

Definition 1 coincides with the ***overlapping grain-error*** model discussed in [15]. We briefly note that since the original model of ***non-overlapping grain-errors*** [10] is a special case of the more general overlapping grain-error model, the code constructions in this paper apply to both models. We compare the upper bounds derived in Section III against existing bounds for the overlapping grain-error model ([15]). For the remainder of the paper, the term grain-error refers to an overlapping grain-error as stated in Definition 1.

Suppose a vector $\boldsymbol{x} \in GF(2)^n$ is stored. Let $\mathcal{B}_{t,G}(\boldsymbol{x})$ be the set of all possible vectors received (the ***error-ball***) given that any t-grain-error may occur in $\boldsymbol{x}$. That is, we define

$$\mathcal{B}_{t,G}(\boldsymbol{x}) = \{\boldsymbol{x} + \boldsymbol{e_x} |\ \boldsymbol{e_x} \text{ is a } t\text{-grain-error}\},$$

and $b_{t,n}(\boldsymbol{x}) = |\mathcal{B}_{t,G}(\boldsymbol{x})|$.

Example 1. *Suppose $\boldsymbol{x} = (0,0,0,1,0)$ was stored. Then, $\mathcal{B}_{1,G}(\boldsymbol{x}) = \{(0,0,0,1,0),(0,0,0,1,1),(0,0,0,0,0)\}$ and $b_{1,5}(\boldsymbol{x}) = 3$. Notice also that $\mathcal{B}_{2,G}(\boldsymbol{x}) = \{(0,0,0,1,0),(0,0,0,1,1),(0,0,0,0,0),(0,0,0,0,1)\}$ and $b_{2,5}(\boldsymbol{x}) = 4$.*

We note that the last vector, $(0,0,0,0,1)$, enumerated in $\mathcal{B}_{2,G}(\boldsymbol{x})$ for Example 1 was an overlapping grain-error in the sense that the grain-errors were adjacent so that the bit in position 4 is both smeared and smearing.

We introduce a new type of error that will be useful in subsequent analysis.

Definition 2. *Let $t \geq 1$ be an integer. Suppose a vector $\boldsymbol{x} \in GF(2)^n$ was stored. Let $\boldsymbol{e_x} = (e_1, \ldots, e_n) \in GF(2)^n$ and suppose the vector $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e_x}$ was received. Then, we say that $\boldsymbol{e_x}$ is a* ***t*-mineral-error for** *$\boldsymbol{x}$ if the following holds:*

1) *$wt(\boldsymbol{e_x}) \leq t$,*
2) *For $2 \leq i \leq n$, if $e_i \neq 0$, then $x_i \neq x_{i-1}$.*

Similar to the grain-error setup, we say that $\boldsymbol{e_x}$ is a t-mineral-error if the vector $\boldsymbol{x}$ is clear from the context. A code that can correct any t-mineral-error will be referred to as a ***t-mineral-error-correcting code***. ***Single-mineral codes*** and ***mineral codes*** are defined analogously as grain codes.

For a given vector $\boldsymbol{x} \in GF(2)^n$, let $\mathcal{B}_{t,M}(\boldsymbol{x})$ denote the error-ball for $\boldsymbol{x}$ given that any t-mineral-error may occur in $\boldsymbol{x}$. That is, we define

$$\mathcal{B}_{t,M}(\boldsymbol{x}) = \{\boldsymbol{x} + \boldsymbol{e_x} |\ \boldsymbol{e_x} \text{ is a } t\text{-mineral-error}\}.$$

A useful consequence of Definition 2 is stated in the following claim.

Claim 1. *Suppose $\mathcal{C}$ is a t-grain-error-correcting code. Then, for any two distinct codewords $\boldsymbol{x} = (x_1, \ldots, x_n), \boldsymbol{y} = (y_1, \ldots, y_n) \in \mathcal{C}$, either*

1) *$x_1 \neq y_1$, or*
2) *$\mathcal{B}_{t,M}(x_2, \ldots, x_n) \cap \mathcal{B}_{t,M}(y_2, \ldots, y_n) = \emptyset$.*

Suppose $\boldsymbol{x} \in GF(2)^n$ and $\mathcal{B}_{t,R}$ denotes the error-ball for ***t random-errors*** (where t random-errors are defined as any binary vector of length n with weight at most t). Then, for any vector $\boldsymbol{x} \in GF(2)^n$, $|\mathcal{B}_{t,R}(\boldsymbol{x})| = \sum_{i=0}^{t} \begin{pmatrix} n \\ i \end{pmatrix}$.

The following lemma follows from the definitions of grain-errors and mineral-errors.

Claim 2. *For any vector $\boldsymbol{x} \in GF(2)^n$, $\mathcal{B}_{t,G}(\boldsymbol{x}) \subseteq \mathcal{B}_{t,M}(\boldsymbol{x}) \subseteq \mathcal{B}_{t,R}(\boldsymbol{x})$.*

We now present some simple results that follow from the structure of grain-errors. Lemmas 1, 2, and 4 will be useful in Section III for obtaining upper bounds on the cardinality of grain codes and Lemma 3 and Claim 3 will be useful for constructing grain codes in Section IV.

A ***run*** is a maximal substring of one or more consecutive identical symbols. We denote the number of runs in a vector $\boldsymbol{x}$ as $r(\boldsymbol{x})$ where $\boldsymbol{x} \in GF(2)^n$.

Lemma 1. *For any vector $\boldsymbol{x}$, $b_{t,n}(\boldsymbol{x}) = \sum_{j=0}^{\min\{t, r(\boldsymbol{x})-1\}} \begin{pmatrix} r(\boldsymbol{x})-1 \\ j \end{pmatrix}$.*

Proof: Suppose a vector $\boldsymbol{x}$ was stored and that it consists of $k = r(\boldsymbol{x})$ runs. By Definition 1, a grain-error can occur only at the boundaries between runs. If there are exactly $k \geq t+1$ runs, there are $k-1$ transitions between runs and therefore $b_{t,n}(\boldsymbol{x}) = \sum_{j=0}^{t} \binom{k-1}{j}$. If there are t or fewer runs (i.e., $k \leq t$), then $b_{t,n}(\boldsymbol{x}) = \sum_{j=0}^{k-1} \binom{k-1}{j}$. ■

The following lemma is a consequence of the smearing effect of a grain-error. Let the map $\Psi : GF(2)^s \to GF(2)^{s-1}$ be defined so that $\Psi(\boldsymbol{z}) = \boldsymbol{z}' = (z'_1, \ldots, z'_{s-1})$ where $z'_i = (z_i + z_{i+1}) \mod 2$ (for $1 \leq i \leq s-1$). Notice that $\Psi(\boldsymbol{z})$ is a linear map and it has a 1 in position i if and only if $z_i \neq z_{i+1}$. Recall that $supp(\boldsymbol{z})$ refers to the set of non-zero indices in $\boldsymbol{z}$ and $wt(\boldsymbol{z})$ refers to the Hamming weight of $\boldsymbol{z}$.

Lemma 2. *For any two vectors $\boldsymbol{x}, \boldsymbol{y} \in GF(2)^n$ if $\boldsymbol{y} \in \mathcal{B}_{t,G}(\boldsymbol{x})$, then $r(\boldsymbol{y}) \leq r(\boldsymbol{x})$ and $b_{t,n}(\boldsymbol{y}) \leq b_{t,n}(\boldsymbol{x})$.*

Proof: For the result to hold, we need to show that for any two vectors $\boldsymbol{x}, \boldsymbol{y} \in GF(2)^n$ where $\boldsymbol{y} \in \mathcal{B}_{t,G}(\boldsymbol{x})$, $r(\boldsymbol{y}) \leq r(\boldsymbol{x})$. If $r(\boldsymbol{y}) \leq r(\boldsymbol{x})$, then from Lemma 1, $b_{t,n}(\boldsymbol{y}) \leq b_{t,n}(\boldsymbol{x})$. Equivalently, we will show that $wt(\Psi(\boldsymbol{y})) \leq wt(\Psi(\boldsymbol{x}))$. Since $\boldsymbol{y} \in \mathcal{B}_{t,G}(\boldsymbol{x})$ we can write $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e_x}$ where $\boldsymbol{e_x}$ is a t-grain-error. Let $\boldsymbol{x}' = \Psi(\boldsymbol{x}), \boldsymbol{e}' = \Psi(\boldsymbol{e_x}), \boldsymbol{y}' = \Psi(\boldsymbol{y})$. By the linearity of the map Ψ, we can write $\boldsymbol{y}' = \boldsymbol{x}' + \boldsymbol{e}'$ and so $wt(\boldsymbol{y}') = wt(\boldsymbol{x}') + wt(\boldsymbol{e}') - 2|supp(\boldsymbol{x}') \cap supp(\boldsymbol{e}')|$. In the following, we show $wt(\boldsymbol{y}') \leq wt(\boldsymbol{x}')$ by proving $|supp(\boldsymbol{x}') \cap supp(\boldsymbol{e}')| \geq \frac{wt(\boldsymbol{e}')}{2}$. The proof will follow by induction on the number of runs of 1s in $\boldsymbol{e_x}$.

We first prove that for any t-grain-error $\boldsymbol{e_x}$ of length n, if $\boldsymbol{e_x}$ has a single run of 1s, then $r(\boldsymbol{y}) \leq r(\boldsymbol{x})$. Suppose then that $\boldsymbol{e_x} = (e_1, \ldots, e_n)$ is a t-grain-error and that $\boldsymbol{e_x}$ contains a single run of 1s. Then $1 \leq wt(\boldsymbol{e}') \leq 2$ since $e_1 = 0$. Suppose further that $\boldsymbol{e}' = (e'_1, \ldots, e'_{n-1})$ has its first 1 at position i where $1 \leq i \leq n-1$. Since i is the location of the first 1 in $\boldsymbol{e}'$, then $e_i \neq e_{i+1}$ and so $e_i = 0, e_{i+1} = 1$ (since $e_1 = 0$). However, if $e_{i+1} = 1$, then $x_i \neq x_{i+1}$ and so both $x'_i = e'_i = 1$. Since $wt(\boldsymbol{e}') \leq 2$, we have just shown that $|supp(\boldsymbol{x}') \cap supp(\boldsymbol{e}')| \geq 1$, and so the base case is complete.

We now assume that for any length-n $\boldsymbol{e_x}$, if $\boldsymbol{e_x}$ has k runs of 1s, then $r(\boldsymbol{y}) \leq r(\boldsymbol{x})$ where $1 \leq k \leq \lfloor \frac{n}{2} \rfloor$. Consider the case where $\boldsymbol{e_x}$ has $k+1$ runs of 1s. Suppose the k-th run of 1s in $\boldsymbol{e_x}$ has its final 1 in position j where $2 \leq j \leq n-2$. Thus, $e_{j+1} = 0$. For shorthand denote $\boldsymbol{e}_1 = (e_1, \ldots, e_{j+1})$, $\boldsymbol{e}_2 = (e_{j+1}, \ldots, e_n)$, $\boldsymbol{x}_1 = (x_1, \ldots, x_{j+1})$, $\boldsymbol{x}_2 = (x_{j+1}, \ldots, x_n)$, $\boldsymbol{e}'_1 = \Psi(\boldsymbol{e}_1)$, $\boldsymbol{e}'_2 = \Psi(\boldsymbol{e}_2)$, $\boldsymbol{x}'_1 = \Psi(\boldsymbol{x}_1)$, and $\boldsymbol{x}'_2 = \Psi(\boldsymbol{x}_2)$. Notice that the vectors $\boldsymbol{e}'$ and $\boldsymbol{x}'$ can be written as the concatenation of two vectors where $\boldsymbol{e}' = (\boldsymbol{e}'_1, \boldsymbol{e}'_2)$ and $\boldsymbol{x}' = (\boldsymbol{x}'_1, \boldsymbol{x}'_2)$ where $\boldsymbol{e}_1$ is a t-grain-error for $\boldsymbol{x}_1$ with k runs of 1s and $\boldsymbol{e}_2$ is a t-grain-error for $\boldsymbol{x}_2$ with a single run of 1s. By the inductive assumption, $|supp(\boldsymbol{x}'_1) \cap supp(\boldsymbol{e}'_1)| \geq \frac{wt(\boldsymbol{e}'_1)}{2}$ and $|supp(\boldsymbol{x}'_2) \cap supp(\boldsymbol{e}'_2)| \geq \frac{wt(\boldsymbol{e}'_2)}{2}$. Combining these two statements gives the desired result that $|supp(\boldsymbol{x}') \cap supp(\boldsymbol{e}')| \geq \frac{wt(\boldsymbol{e}')}{2}$ and so the proof is complete. ■

The following lemma follows from the structure of grain-errors.

Lemma 3. *For any two vectors $\boldsymbol{x}, \boldsymbol{u} \in GF(2)^n$, suppose that for some $1 \leq i \leq n-1$,*

1) $(x_i, x_{i+1}) = (0,0), (u_i, u_{i+1}) = (1,1)$ *or*
2) $(x_i, x_{i+1}) = (1,1), (u_i, u_{i+1}) = (0,0)$.

Then, $\mathcal{B}_{t,G}(\boldsymbol{x}) \cap \mathcal{B}_{t,G}(\boldsymbol{u}) = \emptyset$.

Proof: Let $\boldsymbol{y}_1 = \boldsymbol{x} + \boldsymbol{e_x}$ and $\boldsymbol{y}_2 = \boldsymbol{u} + \boldsymbol{e_u}$. Since $\boldsymbol{x}$ and $\boldsymbol{u}$ differ at position $i+1$ then in order for $\boldsymbol{y}_1 = \boldsymbol{y}_2$, an error must occur at position $i+1$ in either $\boldsymbol{x}$ or $\boldsymbol{u}$ but not both. However, a grain-error can never change the information at position $i+1$ in either $\boldsymbol{x}$ or $\boldsymbol{u}$ since both $\boldsymbol{x}$ and $\boldsymbol{u}$ store the same information in positions i and $i+1$ by the conditions in the statement of the lemma. ■

We now prove the final lemma for this subsection.

Lemma 4. *Suppose $\mathcal{C}$ is a t-grain-error-correcting code of length n with the maximum possible cardinality. Then, $|\mathcal{C}|$ is an even number.*

Proof: Assume, on the contrary, that $\mathcal{C}$ is a t-grain-error-correcting code of length n with an odd number of codewords and $\mathcal{C}$ has maximum possible cardinality. Now consider the code $\mathcal{C}_0$ which consists of all the codewords in $\mathcal{C}$ that start with a 0 and the code $\mathcal{C}_1$ which consists of all the codewords of $\mathcal{C}$ that start with a 1. Notice that since $\mathcal{C}_0$ is a subcode of $\mathcal{C}$, $\mathcal{C}_0$ is a t-grain-error-correcting code. If $|\mathcal{C}| = |\mathcal{C}_0| + |\mathcal{C}_1|$ is an odd number, then $|\mathcal{C}_0| \neq |\mathcal{C}_1|$ and so assume, without loss of generality, that $|\mathcal{C}_1| < |\mathcal{C}_0|$ (the case where $|\mathcal{C}_1| > |\mathcal{C}_0|$ can be treated analogously).

Let $\mathcal{C}'_0$ be the set of vectors that is the result of flipping the first bit of every codeword in $\mathcal{C}_0$. Notice from Claim 1 that since $\mathcal{C}_0$ is a t-grain-error-correcting code for any $\boldsymbol{x} = (x_1, \ldots, x_n), \boldsymbol{y} = (y_1, \ldots, y_n) \in \mathcal{C}_0$ where $\boldsymbol{x} \neq \boldsymbol{y}$, $\mathcal{B}_{t,M}(x_2, \ldots, x_n) \cap \mathcal{B}_{t,M}(y_2, \ldots, y_n) \neq \emptyset$ and so for any $\boldsymbol{v}, \boldsymbol{w} \in \mathcal{C}'_0$ where $\boldsymbol{v} \neq \boldsymbol{w}$, $\mathcal{B}_{t,M}(v_2, \ldots, v_n) \cap \mathcal{B}_{t,M}(w_2, \ldots, w_n) \neq \emptyset$. Thus, for any $\boldsymbol{v}, \boldsymbol{w} \in \mathcal{C}'_0$, we have $\mathcal{B}_{t,G}(\boldsymbol{v}) \cap \mathcal{B}_{t,G}(\boldsymbol{w}) \neq \emptyset$.

Then, $\mathcal{C}_0 \cup \mathcal{C}'_0$ is a t-grain-error-correcting code since each codeword in $\mathcal{C}_0$ differs from every codeword in $\mathcal{C}'_0$ in the first bit. Furthermore, since $|\mathcal{C}'_0| = |\mathcal{C}_0|$,

$$|\mathcal{C}_0 \cup \mathcal{C}'_0| = 2|\mathcal{C}_0| > |\mathcal{C}_0| + |\mathcal{C}_1| = |\mathcal{C}|$$

we arrive at a contradiction. ■

The next claim will be used later in Section IV for constructing grain codes.

Claim 3. *Suppose $\mathcal{C}_M$ is a t-mineral-error-correcting code. Let $\mathcal{C}$ be the code that is the result of prepending an arbitrary bit to the beginning of every codeword in $\mathcal{C}_M$. Then, $\mathcal{C}$ is a t-grain-error-correcting code of size $2|\mathcal{C}_M|$.*

B. Tools for computing upper bounds

In this subsection, we briefly review some of the tools used in Section III for computing a non-asymptotic upper bound on the cardinality of grain-error-correcting codes. We begin by revisiting some of the notation and results from [9].

Definition 3. *A* **hypergraph** $\mathcal{H}$ *is a pair* $(\mathcal{X}, \mathcal{E})$*, where* $\mathcal{X}$ *is a finite set and* $\mathcal{E}$ *is a collection of nonempty subsets of* $\mathcal{X}$ *such that* $\cup_{E\in\mathcal{E}} E = \mathcal{X}$*. The elements of* $\mathcal{E}$ *are called* **hyperedges**.

Definition 4. *A* **matching** *of a hypergraph* $\mathcal{H} = (\mathcal{X}, \mathcal{E})$ *is a collection of disjoint hyperedges* $E_1, \ldots, E_j \in \mathcal{E}$*. The* **matching number** *of* $\mathcal{H}$*, denoted* $\nu(\mathcal{H})$*, is the largest* j *for which such a matching exists.*

As will be described shortly, the following can be interpreted as the dual of the matching of a hypergraph.

Definition 5. *A* **transversal** *of a hypergraph* $\mathcal{H} = (\mathcal{X}, \mathcal{E})$ *is a subset* $T \subseteq \mathcal{X}$ *that intersects every hyperedge in* $\mathcal{E}$*. The* **transversal number** *of* $\mathcal{H}$*, denoted by* $\tau(\mathcal{H})$*, is the smallest size of a transversal.*

Let $\mathcal{H}$ be a hypergraph with vertices $x_1, \ldots, x_n$ and hyperedges $E_1, \ldots, E_m$. The relationships contained within $\mathcal{H}$ can be interpreted through a matrix $A \in \{0,1\}^{n\times m}$, where

$$A(i,j) = \begin{cases} 1 & \text{if } x_i \in E_j, \\ 0 & \text{otherwise,} \end{cases}$$

for $1 \le i \le n, 1 \le j \le m$. Cast in this light, the matching number and the transversal number can be derived using linear optimization techniques.

Lemma 5. *(cf. [9]) The matching number and the transversal number are the solutions of the integer linear programs:*

$$\nu(\mathcal{H}) = \max\{\mathbf{1^T}\boldsymbol{z} | A\boldsymbol{z} \le \mathbf{1}, z_j \in \{0,1\}, 1 \le j \le m\}, \text{ and} \tag{1}$$

$$\tau(\mathcal{H}) = \min\{\mathbf{1^T}\boldsymbol{u} | A^T\boldsymbol{u} \ge \mathbf{1}, u_i \in \{0,1\}, 1 \le i \le n\}, \tag{2}$$

where $\mathbf{1}$ *denotes a column vector of all* 1*s of the appropriate dimension.*

Relaxing the condition that the solutions to the programming problem are comprised of 0s and 1s, we have the following problems:

$$\nu^*(\mathcal{H}) = \max\{\mathbf{1^T}\boldsymbol{z} | A\boldsymbol{z} \le \mathbf{1}, \boldsymbol{z} \ge 0\}, \text{ and} \tag{3}$$

$$\tau^*(\mathcal{H}) = \min\{\mathbf{1^T}\boldsymbol{u} | A^T\boldsymbol{u} \ge \mathbf{1}, \boldsymbol{u} \ge 0\}. \tag{4}$$

Clearly $\nu(\mathcal{H}) \le \nu^*(\mathcal{H})$ and $\tau(\mathcal{H}) \ge \tau^*(\mathcal{H})$. Since (3) and (4) are linear programs, they satisfy strong duality [1] and $\nu^*(\mathcal{H}) = \tau^*(\mathcal{H})$. Thus, combining these inequalities leads us to $\nu(\mathcal{H}) \le \tau^*(\mathcal{H})$ [9].

C. Graph notation

In this subsection, we describe graph notation from [17] that will be used in Section IV-B and Section VI. Let $\mathcal{G} = (V, E)$ be a simple graph; that is, it has undirected edges with no parallel edges and no self-loops. A vertex $\boldsymbol{v}_1 \in V$ is adjacent to another vertex $\boldsymbol{v}_2 \in V$ if there exists an edge between them. The degree of a vertex is the number of its adjacent vertices and the maximum degree of a vertex in $\mathcal{G}$ is denoted $\Delta(\mathcal{G})$.

A ***k-coloring*** is a mapping $\Phi : V \to \{0, 1, \ldots, k-1\}$ of numbers to each vertex such that the same number is never assigned to adjacent vertices. The ***chromatic number*** of a graph, denoted by $\chi(\mathcal{G})$, is the smallest k for which a k-coloring exists. A ***clique*** is a set of vertices in $\mathcal{G}$ that are all adjacent. The size of the largest clique in a graph $\mathcal{G}$ is denoted $\varsigma(\mathcal{G})$. It is known that for a graph $\mathcal{G}$, $\chi(\mathcal{G})$ is such that $\varsigma(\mathcal{G}) \le \chi(\mathcal{G}) \le \Delta(\mathcal{G})+1$ [17]. Each collection of vertices that share the same number (under some fixed k-coloring) is referred to as a ***color class***.

D. Distance metrics and group codes

In this subsection, we introduce some distance metrics that are used in Section IV to construct grain-error-correcting codes. In addition, we define group codes that will serve as the foundation of the single grain-error-correcting codes introduced in Section IV-A.

Definition 6. *Suppose* $\boldsymbol{x}, \boldsymbol{y} \in GF(2)^n$*. Their* **Hamming distance** *is denoted* $d_H(\boldsymbol{x}, \boldsymbol{y}) = |\{i : x_i \ne y_i\}|$.

Definition 7. *Suppose* $\boldsymbol{x} = (x_1, \ldots, x_n), \boldsymbol{y} = (y_1, \ldots, y_n) \in GF(2)^n$*. For* $1 \le i \le n$*,* $N(\boldsymbol{x}, \boldsymbol{y}) = |\{i : x_i > y_i\}|$.

Definition 8. *(cf. [2]) Suppose* $\boldsymbol{x}, \boldsymbol{y}$ *are two vectors in* $GF(2)^n$*. Their* **asymmetric distance** *is denoted* $d_A(\boldsymbol{x}, \boldsymbol{y}) = \max\{N(\boldsymbol{x}, \boldsymbol{y}), N(\boldsymbol{y}, \boldsymbol{x})\}$.

We say that a code $\mathcal{C}$ has ***minimum Hamming distance*** $d_H(\mathcal{C})$ if $d_H(\mathcal{C})$ is the smallest Hamming distance between any two distinct codewords in $\mathcal{C}$. Similarly, we say that a code $\mathcal{C}$ has ***minimum asymmetric distance*** $d_A(\mathcal{C})$ if $d_A(\mathcal{C})$ is the smallest asymmetric distance between any two distinct codewords in $\mathcal{C}$.

Suppose $\mathcal{A}$ is an additive Abelian group of order $n+1$ and suppose $(\tilde{g}_1, \ldots, \tilde{g}_n)$ is a sequence consisting of the distinct non-zero elements of $\mathcal{A}$. For every $a \in \mathcal{A}$, we define a ***group code*** $\tilde{\mathcal{C}}_a^{\mathcal{A}}$ to be

$$\tilde{\mathcal{C}}_a^{\mathcal{A}} = \{\boldsymbol{x} \in GF(2)^n | \sum_{k=1}^{n} x_k \tilde{g}_k = a\}.$$

Without loss of generality, we assume the Abelian groups we deal with in this paper are additive, and that the group operation is denoted as addition. Such a construction was shown in [2] to have $d_H(\tilde{\mathcal{C}}_a^{\mathcal{A}}) \ge d_A(\tilde{\mathcal{C}}_a^{\mathcal{A}}) \ge 2$. We include the following example for clarity.

Example 2. *Let* $\mathcal{A}$ *be the additive Abelian group* $\mathbb{Z}_3$ *so that* $(\tilde{g}_1, \tilde{g}_2) = (1, 2)$*. Then, the group* $\mathcal{A}$ *partitions the space*

$GF(2)^2$ into 3 group codes.

$$\tilde{\mathcal{C}}_0^{\mathbb{Z}_3} = \{(0,0),(1,1)\},$$
$$\tilde{\mathcal{C}}_1^{\mathbb{Z}_3} = \{(1,0)\},$$
$$\tilde{\mathcal{C}}_2^{\mathbb{Z}_3} = \{(0,1)\}.$$

An ***elementary Abelian group*** is a finite Abelian group where every non-identity element in the group has order p, where p is a prime. For shorthand, the elementary Abelian group of size p^r (for a prime p and a positive integer r) is referred to as an ***elementary Abelian p-group*** [14].

E. Discrete Fourier analysis

In this subsection, we briefly review some of the tools that will be used in Section V to derive lower bounds on the cardinalities of code constructions. The notation adopted is similar to the notation used in [11].

Let p be a prime number and suppose ζ_p denotes the complex primitive p-th root of unity and suppose r is some positive integer. Let $\mathcal{A}$ refer to the additive Abelian group $(\mathbb{Z}_p)^r = \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{r \text{ times}}$. The operator $<\boldsymbol{g},\boldsymbol{h}>$ takes two elements $\boldsymbol{g} = (g_1,\ldots,g_r), \boldsymbol{h} = (h_1,\ldots,h_r) \in \mathcal{A}$ and maps them into a complex number as follows

$$<\boldsymbol{g},\boldsymbol{h}> = \prod_{i=1}^{r} (\zeta_p)^{g_i h_i} = (\zeta_p)^{\sum_{i=1}^{r} g_i h_i} = (\zeta_p)^{\boldsymbol{g}^T \cdot \boldsymbol{h}}.$$

Let $f(\boldsymbol{g})$ be any function that maps elements of $\mathcal{A}$ into the complex plane. The ***Fourier transform*** $\hat{f}$ of f is defined as

$$\hat{f}(\boldsymbol{h}) = \sum_{\boldsymbol{g}\in\mathcal{A}} <\boldsymbol{h},-\boldsymbol{g}> f(\boldsymbol{g})$$

and the ***inverse Fourier transform*** is defined as

$$f(\boldsymbol{g}) = \frac{1}{p^r} \sum_{\boldsymbol{h}\in\mathcal{A}} <\boldsymbol{h},\boldsymbol{g}> \hat{f}(\boldsymbol{h}).$$

III. Upper Bounds on Grain-Error Codes

In this section, we use linear programming methods to produce a closed-form upper bound on the cardinality of a t-grain-error-correcting code. The approach is analogous to that found in [9] where upper bounds were computed for the deletion channel and in [8] where upper bounds were derived for the non-overlapping grain-error model. Recall, our objective is to compute upper bounds for the overlapping grain-error model.

The approach is the following. First, the vector space from which codewords are chosen, is projected onto a hypergraph. Then, an approximate solution to a matching problem is derived. Recall that the maximum size of a t-grain-error-correcting-code of length n will be referred to as $M(n,t)$.

Let $\mathcal{H}_{t,n}$ denote the hypergraph for a t-grain-error-correcting code. More formally, let

$$\mathcal{H}_{t,n} = (GF(2)^n, \{\mathcal{B}_{t,G}(\boldsymbol{x}) | \boldsymbol{x} \in GF(2)^n\}).$$

In this graph, the vertices represent candidate codewords and the hyperedges represent vectors that result when t or fewer grain-errors occur in any of the candidate codewords.

As in [9], $\nu^*(\mathcal{H}_{t,n})$ is an upper bound on $M(n,t)$ and will be derived by considering the dual problem defined in (4). The problem is to find a function $w : GF(2)^n \to \mathbb{R}^+$ such that

$$\tau^*(\mathcal{H}_{t,n}) = \min_w \{ \sum_{\boldsymbol{y}\in GF(2)^n} w(\boldsymbol{y}) \}$$

subject to

$$\sum_{\boldsymbol{y}\in\mathcal{B}_{t,G}(\boldsymbol{x})} w(\boldsymbol{y}) \geq 1, \forall \boldsymbol{x} \in GF(2)^n \tag{5}$$

and $w(\boldsymbol{x}) \geq 0, \forall \boldsymbol{x} \in GF(2)^n$.

We are now ready to state the main result of the section.

Theorem 1. *For positive integers n, t where $t < n$,*

$$M(n,t) \leq 2 \sum_{k=0}^{n-1} \binom{n-1}{k} \frac{1}{\sum_{j=0}^{\min\{t,k\}} \binom{k}{j}}.$$

Proof: In order to prove the result, we must assign values for $w(\boldsymbol{y})$ such that the constraint in (5) is satisfied. Let $w(\boldsymbol{y}) = \frac{1}{b_{t,n}(\boldsymbol{y})}$ where $b_{t,n}(\boldsymbol{y})$ is computed as in Lemma 1. Note that

$$\sum_{\boldsymbol{y}\in\mathcal{B}_{t,G}(\boldsymbol{x})} w(\boldsymbol{y}) = \sum_{\boldsymbol{y}\in\mathcal{B}_{t,G}(\boldsymbol{x})} \frac{1}{b_{t,n}(\boldsymbol{y})}.$$

From Lemma 2, for any $\boldsymbol{y} \in \mathcal{B}_{t,G}(\boldsymbol{x})$, $b_{t,n}(\boldsymbol{y}) \leq b_{t,n}(\boldsymbol{x})$, so we have

$$\sum_{\boldsymbol{y}\in\mathcal{B}_{t,G}(\boldsymbol{x})} \frac{1}{b_{t,n}(\boldsymbol{y})} \geq \sum_{\boldsymbol{y}\in\mathcal{B}_{t,G}(\boldsymbol{x})} \frac{1}{b_{t,n}(\boldsymbol{x})} = b_{t,n}(\boldsymbol{x}) \frac{1}{b_{t,n}(\boldsymbol{x})} = 1.$$

The theorem statement now follows from the bound on $\sum_{\boldsymbol{y}\in GF(2)^n} w(\boldsymbol{y})$: Since the number of length-n vectors with k runs is $2\binom{n-1}{k-1}$ and $b_{t,n} = \sum_{j=0}^{\min\{t,k-1\}} \binom{k-1}{j}$ from Lemma 1, we have

$$M(n,t) \leq 2 \sum_{k=1}^{n} \binom{n-1}{k-1} \frac{1}{\sum_{j=0}^{\min\{t,k-1\}} \binom{k-1}{j}},$$

which, after reindexing the parameter k, is the statement in the theorem. ■

Theorem 1 gives an explicit upper bound on $M(n,t)$ for all n and t. However, providing an explicit expression (without summations) is still not easy to derive. In the following, we present non-asymptotic bounds for $t = 1,2,3$. The bounds will then be compared against the existing bounds in [15] for $t = 1$. Note that the overlapping and non-overlapping grain-error models coincide for the case where $t = 1$. The following corollary was also derived in [8] in the context of the non-overlapping grain-error model. It is the result of

combining Theorem 1 for the case where $t = 1$ with Lemma 4. Recall, $M(n,t)$ refers to the maximum size of a t-grain-error-correcting code.

Corollary 1. *For* $n \geq 1$, $M(n,1) \leq 2\lfloor \frac{2^{n+1}-2}{2n} \rfloor$.

In general, it is difficult to compare our bounds to those in [15] since the bounds in [15] require finding a parameter ρ where ρ is the largest integer satisfying $\sum_{k=1}^{\rho} \binom{n-1}{k-1} \sum_{j=0}^{\min(t,k)} \binom{k}{j} \leq 2^{n-1}$. The bounds for $t = 1$ and small n were explicitly derived using the formula in [15] and for all values of $n \leq 20$ the bound in Corollary 1 was tighter (as can be seen in Table I). The bounds in this section have the advantage of being explicit.

For the case of $t = 2$, we make use of the following claims which can be proven using induction. The details are included in Appendix A.

Claim 4. *For* $n \geq 2$,

$$\sum_{k=2}^{n} \frac{1}{k+1} \binom{n}{k} = \frac{1}{n+1} \left(2^{n+1} - 2 - \frac{3n}{2} - \frac{n^2}{2} \right).$$

Claim 5. *For* $n \geq 14$, $\sum_{k=1}^{n} \frac{1}{k} \binom{n}{k} \leq \frac{2^{n+1}}{n-1-\frac{2}{n-5}}$.

We now derive the bound for $M(n,2)$, the maximum size of a 2-grain-error-correcting code, which is non-asymptotic and explicit.

Lemma 6. *For* $n \geq 14$, $M(n,2) \leq 2\left\lfloor \frac{2^{n+2}(2+\frac{2}{n-6})}{2n(n-3)} \right\rfloor$.

Proof: From Theorem 1 we have

$$\begin{aligned} M(n,2) &= 2\sum_{k=0}^{n-1} \binom{n-1}{k} \frac{1}{\sum_{j=0}^{\min\{2,k\}} \binom{k}{j}} \\ &= 2 + n - 1 + 2\sum_{k=2}^{n-1} \binom{n-1}{k} \frac{1}{1+k+\binom{k}{2}} \\ &\leq n + 1 + 4\sum_{k=2}^{n-1} \binom{n-1}{k} \left(\frac{1}{k} - \frac{1}{k+1} \right) \\ &= n + 1 + 4\sum_{k=2}^{n-1} \binom{n-1}{k} \frac{1}{k} - 4\sum_{k=2}^{n-1} \binom{n-1}{k} \frac{1}{k+1}. \end{aligned}$$

From Claims 4 and 5 we have

$$\begin{aligned} M(n,2) &\leq n + 1 + 4\left(\frac{2^n}{n-2-\frac{2}{n-6}} - n + 1 \right) \\ &\quad - \frac{4}{n}\left(2^n - 2 - \frac{3(n-1)}{2} - \frac{(n-1)^2}{2} \right) \\ &= \frac{2^{n+2}}{n-2-\frac{2}{n-6}} - \frac{2^{n+2}}{n} - n + 7 + \frac{4}{n} \\ &\leq \frac{2^{n+2}(2+\frac{2}{n-6})}{n(n-3)}. \end{aligned}$$

From Lemma 4 $M(n,2)$ must be an even integer and so $M(n,2) \leq 2\left\lfloor \frac{2^{n+2}(2+\frac{2}{n-6})}{2n(n-3)} \right\rfloor$. ■

For $t = 3$, the upper bound is stated as a lemma. The details can be found in Appendix A.

Lemma 7. *For* $n \geq 24$,

$$M(n,3) \leq 2\left\lfloor 3 \cdot 2^n \left(\frac{8 + \frac{44}{n-7} + \frac{1}{n} - \frac{2}{(n-2)^2}}{n(n-1)(n-3-\frac{2}{n-7}+\frac{2}{(n-2)^2})} \right) \right\rfloor.$$

IV. Grain-Error Code Constructions

In the previous section, the focus was on upper bounds for grain-error-correcting codes. In this section, we turn to code constructions. We will compare the codes proposed in this section to the upper bounds derived in the previous section.

This section is divided into three subsections. In Section IV-A, we consider a group-theoretic construction for single-grain codes. In Section IV-B, we generalize the construction from IV-A. Using this generalization, Section IV-B identifies better codes that correct single grain-errors for certain code lengths. Section IV-C considers constructions for codes that can correct multiple grain-errors.

A. Single-grain codes

We begin by proving some sufficient conditions for a code to correct a single grain-error. Then, we provide a group-theoretic code construction that satisfies these conditions. The codes presented in this section provide the largest known cardinalities for all code lengths greater than 16.

Combining Lemma 3 with Definition 1, the following claim can be verified. Recall that d_H and d_A refer to the Hamming distance and the asymmetric distance, respectively.

Claim 6. *A code $\mathcal{C}$ is a single-grain code if for every pair of distinct codewords $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}$ one of the following holds:*

1) $d_H(\boldsymbol{x}, \boldsymbol{y}) = 1$ *and* $x_1 \neq y_1$.
2) $d_H(\boldsymbol{x}, \boldsymbol{y}) = 2$ *and for some* $1 < i \leq n-1$,
   a) $(x_i, x_{i+1}) = (0,0), (y_i, y_{i+1}) = (1,1)$ *or*
   b) $(x_i, x_{i+1}) = (1,1), (y_i, y_{i+1}) = (0,0)$.
3) $d_H(\boldsymbol{x}, \boldsymbol{y}) \geq 3$.

We are now ready to state our code construction. For any Abelian group referred to in the subsequent discussion, the identity element will be denoted as 0 and will be referred to as the zero element.

Construction A. *Let $\mathcal{A}$ represent an additive Abelian group of size n. Suppose the sequence $\mathcal{S} = (g_1, g_2, \ldots, g_n)$, which contains the elements of $\mathcal{A}$, is ordered as follows:*

1) $g_1 = 0$,
2) *for any $1 < i \leq n$, the elements g_i and g_i^{-1} (if g_i^{-1} exists) are adjacent.*

For any element $a \in \mathcal{A}$, let

$$\mathcal{C}_a^{\mathcal{A}} = \{\boldsymbol{x} \in GF(2)^n : \sum_{k=1}^{n} x_k g_k = a\}. \tag{6}$$

The following example illustrates Construction A.

Example 3. *Let $\mathcal{A}$ denote the additive Abelian group $\mathbb{Z}_3$. Suppose Construction A is used to create a code where $\mathcal{S} = (g_1, g_2, g_3) = (0, 1, 2)$. Then, the group $\mathcal{A}$ partitions the space $GF(2)^3$ into 3 single-grain codes.*

$$\mathcal{C}_0^{\mathbb{Z}_3} = \{(0,0,0),(1,0,0),(0,1,1),(1,1,1)\},$$
$$\mathcal{C}_1^{\mathbb{Z}_3} = \{(0,1,0),(1,1,0)\},$$
$$\mathcal{C}_2^{\mathbb{Z}_3} = \{(0,0,1),(1,0,1)\}.$$

The correctness of Construction A is proven next.

Theorem 2. *A code $\mathcal{C}_a^{\mathcal{A}}$ created with Construction A is a single-grain code.*

Proof: We will show that $\mathcal{C}_a^{\mathcal{A}}$ is a single-grain code by demonstrating that the conditions listed in Claim 6 hold for any pair of distinct codewords $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}_a^{\mathcal{A}}$. Let $\tilde{\mathcal{C}}_a^{\mathcal{A}}$ be the group code created by using the same group and element a as in $\mathcal{C}_a^{\mathcal{A}}$ so that $\tilde{\mathcal{C}}_a^{\mathcal{A}}$ has length $n-1$, and $\tilde{\mathcal{C}}_a^{\mathcal{A}}$ is obtained by shortening the codewords of $\mathcal{C}_a^{\mathcal{A}}$ on the first bit (i.e., by removing x_1, which multiplies $g_1 = 0$). Recall from Section II-D that since $\tilde{\mathcal{C}}_a^{\mathcal{A}}$ is a group code, $d_H(\tilde{\mathcal{C}}_a^{\mathcal{A}}) \geq d_A(\tilde{\mathcal{C}}_a^{\mathcal{A}}) \geq 2$.

Suppose $d_H(\boldsymbol{x}, \boldsymbol{y}) = 1$. Then, since $d_H(\tilde{\mathcal{C}}_a^{\mathcal{A}}) \geq 2$, it follows that if $d_H(\boldsymbol{x}, \boldsymbol{y}) = 1$, then $\boldsymbol{x}$ and $\boldsymbol{y}$ differ only in the first bit and so condition 1) from Claim 6 holds.

Suppose $d_H(\boldsymbol{x}, \boldsymbol{y}) = 2$. Since $d_H(\tilde{\mathcal{C}}_a^{\mathcal{A}}) \geq 2$, $\boldsymbol{x}$ and $\boldsymbol{y}$ do not differ in the first position, and there are two distinct indices i, j ($2 \leq i, j \leq n$) where $x_i \neq y_i$ and $x_j \neq y_j$. Suppose, without loss of generality, that $N(\boldsymbol{x}, \boldsymbol{y}) = 2$ and so $x_i = x_j = 1$. Therefore, $g_i + g_j = 0$, or $g_j = g_i^{-1}$. However, by condition 2) in Construction A, we have $|j - i| = 1$ and so condition 2) from Claim 6 holds.

If $d_H(\boldsymbol{x}, \boldsymbol{y})$ is not equal to 1 or 2 then $d_H(\boldsymbol{x}, \boldsymbol{y}) \geq 3$ and so condition 3) of Claim 6 holds. ■

The following corollary follows from the proof of Theorem 2 and Claim 1.

Corollary 2. *Let $\mathcal{C}_a^{\mathcal{A}}$ be a single-grain code created according to Construction A. Let $\tilde{\mathcal{C}}_a^{\mathcal{A}}$ be the group code that is the result of shortening the codewords in $\mathcal{C}_a^{\mathcal{A}}$ on the first bit. Then $\tilde{\mathcal{C}}_a^{\mathcal{A}}$ is a single-mineral code.*

The following corollary provides upper and lower bounds on $|\mathcal{C}_a^{\mathcal{A}}|$.

Corollary 3. *Suppose $\mathcal{A}$ is an Abelian group of size n and $a \in \mathcal{A}$. Then, for a code $\mathcal{C}_a^{\mathcal{A}}$ created according to Construction A, $|\mathcal{C}_a^{\mathcal{A}}| \leq |\mathcal{C}_0^{\mathcal{A}}|$. Furthermore,*

$$\frac{2^n}{n} \leq |\mathcal{C}_0^{\mathcal{A}}| \leq \frac{2^n}{n} + \frac{(n-1) \cdot 2^{n/3}}{n}.$$

Equality holds on the left if and only if $|\mathcal{A}|$ is a power of two. Equality holds on the right if and only if $\mathcal{A}$ is an elementary Abelian 3-group.

Proof: Since Construction A concatenates an arbitrary bit with a group code, it follows that if the underlying group code of length $n' = n - 1$ has cardinality $|\tilde{\mathcal{C}}_a^{\mathcal{A}}|$, then the code $\mathcal{C}_a^{\mathcal{A}}$ created using the previous construction has $2|\tilde{\mathcal{C}}_a^{\mathcal{A}}|$ codewords. Then, since $|\tilde{\mathcal{C}}_a^{\mathcal{A}}| \leq |\tilde{\mathcal{C}}_0^{\mathcal{A}}|$ ([2], Theorem 9), $|\mathcal{C}_a^{\mathcal{A}}| \leq |\mathcal{C}_0^{\mathcal{A}}|$. Furthermore, from ([11], Corollary 2) $|\tilde{\mathcal{C}}_0^{\mathcal{A}}| \leq \frac{1}{n'+1}\left(2^{n'} + n' 2^{n'/3}\right)$ with equality if and only if $\mathcal{A}$ is an elementary Abelian 3-group. From ([11], Corollary 1), $|\tilde{\mathcal{C}}_0^{\mathcal{A}}| = \frac{2^{n'}}{n'+1}$ if and only if $n'+1$ is a power of 2. Multiplying $|\tilde{\mathcal{C}}_0^{\mathcal{A}}|$ by 2 and replacing $n = n' + 1$ then gives the result in the corollary. ■

In [15], a single-grain code construction was given that produced codes of length $n = 2^m - 1$ with $\frac{2^n}{n+1} + 2^{\frac{(n-1)}{2}}$ codewords where m is a positive integer. In [10], a single-grain code construction was enumerated that resulted in codes of length n where $n = 2^r$ (where r is a positive integer), that contained $\frac{2^n}{n}$ codewords.

Our construction extends for any n (via the set $\mathcal{A} = \mathbb{Z}_n$). When n is a power of 2, Construction A produces codes with the same cardinality as [10]. Furthermore, for codes of length n where n is not a power of 2, Construction A provides codebooks with cardinalities strictly greater than $\frac{2^n}{n}$ by Corollary 3.

Since, for large n,

$$\frac{2^n}{n} > \frac{2^n}{n+1} + 2^{\frac{n-1}{2}},$$

Construction A improves upon the state of the art when n is not a power of 2 and $n \geq 15$.

In the next subsection, we provide a generalization of Construction A. We then derive constructions for single-grain codes that have larger cardinalities and extend the ideas to codes capable of correcting more than a single grain-error.

B. Improved grain codes using mappings

In [5], the authors make the observation that a single-asymmetric error-correcting code (and in particular a group code) can be constructed by defining a code over pairs of binary elements. Consider the map $\Gamma : \{0,1\}^2 \to GF(3)$, which is defined as follows:

$$(0,0) \to 0, (0,1) \to 1, (1,0) \to 2, (1,1) \to 0. \tag{7}$$

Note that the map is not one-to-one since both $(0,0)$ and $(1,1)$ map to 0. If the map Γ is applied to a binary vector of even length then it is simply applied to each pair of consecutive elements at a time (i.e., $\Gamma(0,1,0,0) = (\Gamma(0,1), \Gamma(0,0))$). Furthermore, if the Γ map is applied to a set of vectors it returns a set of ternary vectors that are the result of applying the map to each vector in the set. Using this map, codes that correct asymmetric errors were proposed in [5]. In the following, we illustrate how to generalize the ideas from [5] (by using different mappings) to correct grain-errors.

Let $\mathcal{G}_{t,m} = (V, E)$ denote a simple graph (see Section II-C) where $V = GF(2)^m$. That is, the vertices of $\mathcal{G}_{t,m}$ are the the vectors from $GF(2)^m$. For any $\boldsymbol{x}, \boldsymbol{y} \in V$, $(\boldsymbol{x}, \boldsymbol{y}) \in E$ if $\mathcal{B}_{t,M}(\boldsymbol{x}) \cap \mathcal{B}_{t,M}(\boldsymbol{y}) \neq \emptyset$. Recall from Section II-C, a mapping $\Phi_{t,m} : GF(2)^m \to \{0, 1, \ldots, p-1\}$ is a p-coloring if it assigns

different numbers to adjacent vertices. If the input to $\Phi_{t,m}$ is a vector of length mn, then the map is applied to each collection of m consecutive bits at a time. For example, if $m = 3$, then $\Phi_{t,3}(0,0,0,1,0,1) = (\Phi_{t,3}(0,0,0)\ \Phi_{t,3}(1,0,1))$.

Construction B. *Suppose p is a prime number and $\Phi_{t,m} : GF(2)^m \to \{0,1,\ldots,p-1\}$ is a p-coloring on $\mathcal{G}_{t,m}$. Let $\mathcal{C}_t$ be a t-random-error-correcting code over $GF(p)$ of length n. Then,*

$$\mathcal{C} = \{\boldsymbol{x} \in GF(2)^{mn} : \Phi_{t,m}(\boldsymbol{x}) \in \mathcal{C}_t\}. \tag{8}$$

Remark 1. *If $\mathcal{C}$ is a code created according to Construction B, then the map $\Phi_{t,m}$ can be interpreted as mapping the color classes of a p-coloring onto the symbols of a non-binary code $\mathcal{C}_t$. This interpretation will be useful in Section VI.*

We now provide an example of a code created with Construction B.

Example 4. *Let the map Γ be as defined in (7). Note, from Lemma 3, that the map Γ is actually a coloring on $\mathcal{G}_{t,2}$ where the set of vectors $GF(2)^2$ are partitioned into color classes as follows:*

1) $\{(0\ 0), (1\ 1)\}$,
2) $\{(1\ 0)\}$,
3) $\{(0\ 1)\}$.

Let $\mathcal{C}_t$ be a t-random-error-correcting code over $GF(3)$ of length n. Then the set of vectors

$$\mathcal{C} = \{\boldsymbol{x} \in GF(2)^{2n} : \Gamma(\boldsymbol{x}) \in \mathcal{C}_t\} \tag{9}$$

is a code created according to Construction B.

Remark 2. *We note that when $\mathcal{C}_t$ is a single-random-error-correcting code, a code constructed according to Example 4 coincides with the ternary construction from [5] proposed in the context of asymmetric errors.*

The following theorem shows that the code $\mathcal{C}$ created in Example 4 is a t-mineral-error-correcting code.

Theorem 3. *Let $\mathcal{C}_t$ be a t-random-error-correcting code. Suppose $\mathcal{C}$ is a code created according to Construction B with $\mathcal{C}_t$ as the constituent code. Then, $\mathcal{C}$ is a t-mineral-error-correcting code.*

Proof: The result will be proven by showing that for any codewords $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}$ where $\boldsymbol{x} \neq \boldsymbol{y}$, $\mathcal{B}_{t,M}(\boldsymbol{x}) \cap \mathcal{B}_{t,M}(\boldsymbol{y}) = \emptyset$. Consider two codewords $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}$ such that $\boldsymbol{x} \neq \boldsymbol{y}$ and $\Phi_{t,m}(\boldsymbol{x}) = \Phi_{t,m}(\boldsymbol{y})$. There are two cases to consider: either 1) $\Phi_{t,m}(\boldsymbol{x}) = \Phi_{t,m}(\boldsymbol{y})$ or 2) $\Phi_{t,m}(\boldsymbol{x}) \neq \Phi_{t,m}(\boldsymbol{y})$. Recall that, by construction, $\Phi_{t,m}(\boldsymbol{x}), \Phi_{t,m}(\boldsymbol{y}) \in \mathcal{C}_t$.

Suppose $\Phi_{t,m}(\boldsymbol{x}) = \Phi_{t,m}(\boldsymbol{y})$. Then, since $\boldsymbol{x} \neq \boldsymbol{y}$, there exists an index i where $1 \leq i \leq n$ such that $\Phi_{t,m}(x_{(i-1)m+1}, \ldots, x_{im}) = \Phi_{t,m}(y_{(i-1)m+1}, \ldots, y_{im})$ but $(x_{(i-1)m+1}, \ldots, x_{im}) \neq (y_{(i-1)m+1}, \ldots, y_{im})$. For shorthand, let $\boldsymbol{v}_1 = (x_{(i-1)m+1}, \ldots, x_{im})$ and $\boldsymbol{v}_2 = (y_{(i-1)m+1}, \ldots, y_{im})$. Since $\Phi_{t,m}(\boldsymbol{v}_1) = \Phi_{t,m}(\boldsymbol{v}_2)$, the vectors $\boldsymbol{v}_1, \boldsymbol{v}_2$ map to the same color class under $\Phi_{t,m}$, which implies that $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$ are not adjacent in $\mathcal{G}_{t,m}$. By definition, if $\boldsymbol{v}_1, \boldsymbol{v}_2$ are not adjacent in $\mathcal{G}_{t,m}$, $\mathcal{B}_{t,M}(\boldsymbol{v}_1) \cap \mathcal{B}_{t,M}(\boldsymbol{v}_2) = \emptyset$. Thus, for any t-mineral-errors (of length m) $\boldsymbol{e}_{\boldsymbol{v}_1}, \boldsymbol{e}_{\boldsymbol{v}_2}$, we have $\boldsymbol{v}_1 + \boldsymbol{e}_{\boldsymbol{v}_1} \neq \boldsymbol{v}_2 + \boldsymbol{e}_{\boldsymbol{v}_2}$. Then, there do not exist any t-mineral-errors $\boldsymbol{e}_{\boldsymbol{x}}, \boldsymbol{e}_{\boldsymbol{y}}$ such that $\boldsymbol{x} + \boldsymbol{e}_{\boldsymbol{x}} = \boldsymbol{y} + \boldsymbol{e}_{\boldsymbol{y}}$. Thus, $\mathcal{B}_{t,M}(\boldsymbol{x}) \cap \mathcal{B}_{t,M}(\boldsymbol{y}) = \emptyset$.

Suppose now that $\Phi_{t,m}(\boldsymbol{x}) \neq \Phi_{t,m}(\boldsymbol{y})$. Then, since $\Phi_{t,m}(\boldsymbol{x}), \Phi_{t,m}(\boldsymbol{y}) \in \mathcal{C}_t$, there exists a set of at least $2t+1$ indices from $\{1, 2, \ldots, n\}$, denoted as $\mathcal{I}$, such that $\forall j \in \mathcal{I}$, $\Phi_{t,m}(x_{(j-1)m+1}, \ldots, x_{jm}) \neq \Phi_{t,m}(y_{(j-1)m+1}, \ldots, y_{jm})$. Since $\Phi_{t,m}(x_{(j-1)m+1}, \ldots, x_{jm}) \neq \Phi_{t,m}(y_{(j-1)m+1}, \ldots, y_{jm})$, $d_H((x_{(j-1)m+1}, \ldots, x_{jm}), (y_{(j-1)m+1}, \ldots, y_{jm})) \geq 1$ for every $j \in \mathcal{I}$ and so $d_H(\boldsymbol{x}, \boldsymbol{y}) \geq 2t+1$. Thus, $\mathcal{B}_{t,R}(\boldsymbol{x}) \cap \mathcal{B}_{t,R}(\boldsymbol{y}) = \emptyset$ where $\mathcal{B}_{t,R}$ denotes the error-ball for t random-errors (as discussed in Section II-A). From Claim 2, then $\mathcal{B}_{t,M}(\boldsymbol{x}) \cap \mathcal{B}_{t,M}(\boldsymbol{y}) = \emptyset$ as well and the proof is complete. ■

According to Theorem 3, the code from Example 4 is a t-mineral-error-correcting code. Corollary 4 follows from Claim 3.

Corollary 4. *Let $\mathcal{C}'$ be a t-mineral-error-correcting code of length mn created according to Construction B. Then,*

$$\mathcal{C} = \{\boldsymbol{x} \in GF(2)^{mn+1} : (x_2, \ldots, x_{mn+1}) \in \mathcal{C}'\}$$

is a t-grain-error-correcting code.

Although Construction B provides a method to construct t-mineral-error-correcting codes, it is not straightforward to compute the sizes of the resulting codes because the color classes of the map $\Phi_{t,m}$ are not always of the same size. As a starting point, in this subsection we only consider single-mineral codes created using Construction B with the map Γ as described in Example 4. Even with the simple map Γ, computing the cardinalities of the resulting codes from Construction B is not straightforward. In the following subsection, we analyze the codes from Example 4 for arbitrary t.

Recall that from Remark 2, the single asymmetric error-correcting codes proposed in [5] (using the ternary construction) are a special case of Construction B. Therefore, the codes from (Table II, column 4, [5]) are single-mineral codes. Therefore, we can obtain new single-grain codes by appending an information bit to these codes. The cardinalities displayed in the column titled 'Current Lower Bound' (second column) of Table I (shown below) for $9 \leq n \leq 15$ are the result of this operation. Note that the codes enumerated from [5] were the result of a computerized search and to limit the search space, the search was only carried out on codes of length at most 15. For $n \geq 16$ the cardinalities in the second column of Table I (marked in bold) can be obtained from Construction A using the group codes found in Table 1 in [2]. The first column in Table I shows the cardinalities of the largest possible codebooks using constructions from [10] and

TABLE I
UPPER AND LOWER BOUNDS FOR SINGLE GRAIN-ERROR-CORRECTING CODES

Length	Previous Lower Bound	Current Lower Bound	Upper Bound
3	4 [15]	4 [15]	4 [15]
4	6 [15]	6 [15]	6 [15]
5	8 [15]	8 [15]	8 [15]
6	16 [15]	16 [15]	16 [15]
7	26 [15]	26 [15]	26 [15]
8	44[15]	44 [15]	44 [15]
9	44 [15]	**64**	112
10	64 [10]	**110**	204
11	128 [10]	**210**	372
12	256 [10]	**360**	682
13	512 [10]	**702**	1260
14	1024 [10]	**1200**	2340
15	2176 [15]	**2400**	4368
16	4096 [10]	**4096**	8190
17	4096 [10]	**7712**	15420
18	8192 [10]	**14592**	29126
19	16384 [10]	**27596**	55188
20	32768 [10]	**52432**	104856

[15]. The third column in the table is the upper bound from Corollary 1 (Section III), which can also be found in [8].

C. Multiple grain-error codes using the Γ coloring

In this subsection, multiple grain-error-correcting codes are studied. In particular, we consider an alternative interpretation of the codes from Example 4. Using this interpretation, we derive a lower bound on the size of a mineral code created according to Example 4 for the case where the code $\mathcal{C}_t$ is linear.

Notice that if the Hamming weight enumerator for the constituent code $\mathcal{C}_t$ in Example 4 is given, then the size of the code $\mathcal{C}$ can be expressed as a function of the Hamming weight enumerator for $\mathcal{C}_t$. We denote the Hamming weight enumerator of a code $\mathcal{C}$ as $W_{\mathcal{C}}(x,z) = \sum_{i=0}^{n} W_{i,n-i} z^i x^{n-i}$ where $W_{i,n-i}$ represents the number of codewords in $\mathcal{C}$ whose Hamming weight is i. The following lemma is similar to Theorem 9 in [5] and so the proof is omitted.

Lemma 8. *Let $\mathcal{C}_t$ be a ternary code of length n used in Example 4 with Hamming weight enumerator*

$$\mathcal{W}_{\mathcal{C}_t}(x,z) = \sum_{i=0}^{n} W_{i,n-i} z^i x^{n-i}.$$

Then, the resulting mineral-error-correcting code $\mathcal{C}$ has cardinality $|\mathcal{C}| = W_{\mathcal{C}_t}(1,2)$. Prepending an additional information bit to every codeword in $\mathcal{C}$ results in a grain-error-correcting code with cardinality $2|\mathcal{C}|$.

Remark 3. *Note that in general the weight enumerator for any t-random-error-correcting ternary code $\mathcal{C}_t$ is not necessarily known.*

Using Lemma 8, the cardinalities of grain codes created according to Example 4 with odd lengths between 11 and 29 are displayed in Table II. Each entry consists of 3 numbers (or entries) delimited by a '/'. Since for $1 < t < n$ there are no existing grain-error-correcting codebooks to compare with, we naively constructed a t-grain-error-correcting code by prepending an additional information bit to the start of a t-random-error-correcting code.

The first entry (from each triplet) in Table II is the cardinality of the largest linear t-random-error-correcting binary code found in [16] of length $n-1$ prepended by an additional information bit. The second entry is the cardinality of a code created from Example 4. This number was computed from the known weight enumerators of the largest known linear ternary codes from [16] prepended by an additional information bit. The third entry is the non-asymptotic upper bound from Theorem 1 and Lemma 4.

In the following, we provide a variation of the codes from Example 4 in order to provide an explicit lower bound on the size of codes created as in Example 4 when $\mathcal{C}_t$ is linear. This will be studied in more detail in Section V.

Construction C. *Let r, ℓ be positive integers where $r < \ell$. Let $H' = (\boldsymbol{h}'_1, \ldots, \boldsymbol{h}'_\ell)$ be an $r \times \ell$ parity check matrix of a ternary code $\mathcal{C}'$ of length ℓ that can correct up to t random-errors (where each $\boldsymbol{h}'_i$ represents the ith column in H', $1 \le i \le \ell$). Let H be an $r \times 2\ell$ ternary matrix,*

$$H = (\boldsymbol{h}_1, \ldots, \boldsymbol{h}_{2\ell}) = (2\boldsymbol{h}'_1, \boldsymbol{h}'_1, 2\boldsymbol{h}'_2, \boldsymbol{h}'_2, \ldots, 2\boldsymbol{h}'_\ell, \boldsymbol{h}'_\ell).$$

Let $\boldsymbol{a}$ be an arbitrary element in $GF(3)^r$. Then,

$$\mathcal{C}_{\boldsymbol{a}} = \{\boldsymbol{x} \in GF(2)^{2\ell} : H\boldsymbol{x} = \boldsymbol{a}\}, \tag{10}$$

where the vector operations are performed in the vector space $GF(3)^r$.

The following lemma will be useful in proving the correctness of Construction C.

Lemma 9. *Let r, ℓ be positive integers where $r < \ell$ and let the matrices H', H be as in Construction C. Then for any $\boldsymbol{x} \in GF(2)^{2\ell}$, $H \cdot \boldsymbol{x} = H' \cdot \Gamma(\boldsymbol{x})$.*

Proof: For any $\boldsymbol{x} = (x_1, \ldots, x_{2\ell}) \in GF(2)^{2\ell}$ we have $H \cdot \boldsymbol{x} = \sum_{i=1}^{2\ell} \boldsymbol{h}_i \cdot x_i$ where $\boldsymbol{h}_i \in GF(3)^r$. Consider the quantity

$$\begin{aligned} H \cdot \boldsymbol{x} &= \sum_{i=1}^{2\ell} \boldsymbol{h}_i \cdot x_i \\ &= \sum_{j=1, j \text{ odd}}^{2\ell-1} (\boldsymbol{h}_j, \boldsymbol{h}_{j+1}) \cdot (x_j, x_{j+1})^T \\ &= \sum_{j=1, j \text{ odd}}^{2\ell-1} (2\boldsymbol{h}'_{\lceil \frac{j}{2} \rceil}, \boldsymbol{h}'_{\lceil \frac{j}{2} \rceil}) \cdot (x_j, x_{j+1})^T. \end{aligned} \tag{11}$$

There are the 4 possibilities for (x_j, x_{j+1}):

1) $(x_j, x_{j+1}) = (0,0)$,
2) $(x_j, x_{j+1}) = (0,1)$,
3) $(x_j, x_{j+1}) = (1,0)$,
4) $(x_j, x_{j+1}) = (1,1)$.

TABLE II
CARDINALITIES OF GRAIN-ERROR-CORRECTING CODES

Length	$t=2$	$t=3$	$t=4$	$t=5$
11	16/68/84	-	-	-
13	32/132/238	-	-	-
15	128/312/704	32/260/400	-	-
17	512/836/2152	64/516/1066	-	-
19	1024/2636/6780	256/1028/2946	16/1028/1928	-
21	4096/9376/21902	1024/2144/8490	64/2052/4940	-
23	16384/35648/72190	4096/4688/24786	128/4100/13050	32/4100/9370
25	32768/49024/241978	8192/8896/74902	256/8320/35510	64/8196/23382
27	131072/190912/822696	16384/20808/231538	1024/17216/99330	256/16388/59814
29	524288/747520/2831212	32768/41616/729924	2048/34096/285020	512/32772/156924

If any of conditions $1)-4)$ hold, then it can be verified that when j is odd, we have (where Γ is as defined in (7))

$$(2\boldsymbol{h}'_{\lceil \frac{j}{2} \rceil}, \boldsymbol{h}'_{\lceil \frac{j}{2} \rceil}) \cdot (x_j, x_{j+1})^T = \boldsymbol{h}'_{\lceil \frac{j}{2} \rceil} \cdot \Gamma(x_j, x_{j+1}).$$

Then, continuing from (11),

$$\begin{aligned} H \cdot \boldsymbol{x} &= \sum_{j=1, j \text{ odd}}^{2\ell-1} (2\boldsymbol{h}'_{\lceil \frac{j}{2} \rceil}, \boldsymbol{h}'_{\lceil \frac{j}{2} \rceil}) \cdot (x_j, x_{j+1})^T \\ &= \sum_{j=1, j \text{ odd}}^{2\ell-1} \boldsymbol{h}'_{\lceil \frac{j}{2} \rceil} \cdot \Gamma(x_j, x_{j+1}) \\ &= \sum_{k=1}^{\ell} \boldsymbol{h}'_k \cdot \Gamma(x_{2k-1}, x_{2k}) \\ &= H' \cdot \Gamma(\boldsymbol{x}). \end{aligned}$$

■

We now prove the correctness of Construction C.

Theorem 4. *Suppose $\mathcal{C}_{\boldsymbol{a}}$ is a code created according to Construction C. Then, $\mathcal{C}_{\boldsymbol{a}}$ is a t-mineral-error-correcting code.*

Proof: Let H' be a parity check matrix of dimension r (where $r \leq \ell$) for the code $\mathcal{C}'$ of length ℓ. For any $\boldsymbol{a} \in \mathcal{A}$, let $\mathcal{C}'_{\boldsymbol{a}} = \{\boldsymbol{x} \in GF(3)^\ell : H' \cdot \boldsymbol{x} = \boldsymbol{a}\}$. Notice that for any $\boldsymbol{a} \in \mathcal{A}$, $\mathcal{C}'_{\boldsymbol{a}}$ is a ternary t-random-error-correcting code. Recall from Construction C that $\mathcal{C}_{\boldsymbol{a}} = \{\boldsymbol{x} \in GF(2)^{2\ell} : H\boldsymbol{x} = \boldsymbol{a}\}$ where $H = (2\boldsymbol{h}'_1, \boldsymbol{h}'_1, 2\boldsymbol{h}'_2, \boldsymbol{h}'_2, \ldots, 2\boldsymbol{h}_\ell, \boldsymbol{h}'_\ell) = (\boldsymbol{h}_1, \ldots, \boldsymbol{h}_{2\ell})$ (and each $\boldsymbol{h}_i, \boldsymbol{h}'_j$ denotes a column in H or H', respectively for $1 \leq i \leq 2\ell$ and $1 \leq j \leq \ell$).

From Lemma 9, for any vector $\boldsymbol{x} \in GF(2)^n$, $H \cdot \boldsymbol{x} = H' \cdot \Gamma(\boldsymbol{x})$. Therefore, it follows that $H \cdot \boldsymbol{x} = \boldsymbol{a}$ if and only if $H' \cdot \Gamma(\boldsymbol{x}) = \boldsymbol{a}$. Then, we can write $\mathcal{C}_{\boldsymbol{a}} = \{\boldsymbol{x} \in GF(2)^n : \Gamma(\boldsymbol{x}) \in \mathcal{C}'_{\boldsymbol{a}}\}$. Since $\mathcal{C}'_a$ is a t-random-error-correcting code, $\mathcal{C}_{\boldsymbol{a}}$ is a t-mineral-error-correcting code by Example 4 and Theorem 3. ■

Using the interpretation of the codes from Example 4 provided by Construction C, we now state a simple lower bound on the size of a code created as in Example 4. Recall from Theorem 4, Construction C is a special case of the codes from Example 4. The lower bound in Corollary 5 will be improved in the next section.

Recall for the following corollary that $\mathcal{A}$ denotes an Abelian group.

Corollary 5. *Let $\mathcal{C}'$ be a t-random-error-correcting ternary code of length $\ell = \frac{n}{2}$ (where n is even) with a parity check matrix H' of dimension r. Then there exists an $\boldsymbol{a} \in \mathcal{A}$, such that the code $\mathcal{C}_{\boldsymbol{a}}$ created according to Construction C of length n with the constituent code $\mathcal{C}'$ satisfies $|\mathcal{C}_{\boldsymbol{a}}| \geq \frac{2^n}{3^r}$.*

Proof: Notice that each of the $2^{2\ell}$ vectors from $GF(2)^{2\ell}$ will map to exactly one code $\mathcal{C}_{\boldsymbol{a}}$ as in (10). Thus, the matrix H partitions the space $GF(2)^{2\ell}$ into $|\mathcal{A}|$ non-overlapping codes $\mathcal{C}_{\boldsymbol{a}_1}, \mathcal{C}_{\boldsymbol{a}_2}, \mathcal{C}_{\boldsymbol{a}_3}, \ldots, \mathcal{C}_{\boldsymbol{a}_{3^r}}$ where each $\boldsymbol{a}_i \in \mathcal{A}$ for $1 \leq i \leq 3^r$. By the pigeonhole principle, there must exist a code with cardinality at least $\frac{2^{2\ell}}{|\mathcal{A}|} = \frac{2^n}{3^r}$. ■

In the next section, we use Fourier analysis to improve the lower bound on $\mathcal{C}_{\boldsymbol{a}}$ from Construction C.

V. AN IMPROVEMENT ON THE LOWER BOUNDS ON THE CARDINALITY OF GRAIN AND MINERAL CODES WHEN $t \geq 2$

In this section, we improve the lower bound from the previous section for the cardinality of a t-mineral-error-correcting code created according to Construction C. The approach will be similar to [11], where the cardinalities of the Constantin-Rao codes [2] were derived using discrete Fourier analysis.

Let $\mathcal{A}$ be the additive Abelian group of $GF(3)^r$. Let $\mathcal{C}_{\boldsymbol{a}}$ denote a code created using Construction C where as before $\boldsymbol{a}$ is an element from $\mathcal{A}$ used in the construction. Suppose further that $\mathcal{C}'$ is a ternary code of length ℓ with a parity check matrix H' that can correct up to t random-errors where $\mathcal{C}'$ is the constituent code used in Construction C. For $1 \leq i \leq \ell$, recall from the construction that $\boldsymbol{h}'_i$ refers to the ith column of H' and that for $1 \leq j \leq 2\ell$, $\boldsymbol{h}_j$ refers to the jth column of H where $H = (\boldsymbol{h}_1, \ldots, \boldsymbol{h}_{2\ell}) = (2\boldsymbol{h}'_1, \boldsymbol{h}'_1, 2\boldsymbol{h}'_2, \boldsymbol{h}'_2, \ldots, 2\boldsymbol{h}'_\ell, \boldsymbol{h}'_\ell)$.

For $\boldsymbol{x} = (x_1, \ldots, x_{2\ell}) \in GF(2)^{2\ell}$, consider the mapping $\gamma : GF(2)^{2\ell} \to \mathcal{A}$ defined as

$$\gamma(\boldsymbol{x}) = H \cdot \boldsymbol{x} = \sum_{j=1}^{2\ell} x_j \boldsymbol{h}_j = \sum_{i=1}^{\ell} x_{2i} \boldsymbol{h}'_i + \sum_{k=1}^{\ell} 2x_{2k-1} \boldsymbol{h}'_k. \tag{12}$$

In order to compute $|\mathcal{C}_{\boldsymbol{a}}|$, we count the number of times each element $\boldsymbol{a} \in \mathcal{A}$ is covered by some vector $\boldsymbol{x} \in GF(2)^{2\ell}$

through γ. Let $f : \mathcal{A} \to \mathbb{N}$ where

$$f(\boldsymbol{a}) = |\{\boldsymbol{x} \in GF(2)^{2\ell} : \gamma(\boldsymbol{x}) = H \cdot \boldsymbol{x} = \boldsymbol{a}\}|. \tag{13}$$

We state the following claim for clarity. Recall, $M(n,t)$ refers to the maximum size of a t-grain-error-correcting code of length n.

Claim 7. *Let n, ℓ be positive integers such that $n = 2\ell+1$. Let $\mathcal{C}_{\boldsymbol{a}}$ be a code of length 2ℓ created according to Construction C where $\boldsymbol{a} \in \mathcal{A}$. Then, $|\mathcal{C}_{\boldsymbol{a}}| = f(\boldsymbol{a})$ and $M(n,t) \geq 2|\mathcal{C}_{\boldsymbol{a}}| = 2f(\boldsymbol{a})$.*

We are now ready to derive lower bounds on the sizes of codes created from Construction C using Fourier analysis. The following lemma will be used in the proof of Theorem 5. Recall from Section II-E, for $\boldsymbol{a}, \boldsymbol{b} \in \mathcal{A}$,

$$<\boldsymbol{a}, \boldsymbol{b}> = \prod_{i=1}^{r} (\zeta_3)^{a_i b_i} = (\zeta_3)^{\sum_{i=1}^{r} a_i b_i} = (\zeta_3)^{\boldsymbol{a}^T \cdot \boldsymbol{b}}$$

where ζ_3 is a third root of unity. In the remainder, for some positive integer k, $(\zeta_3)^k$ will be written as ζ_3^k.

In the next lemma, we make use of the following function. Let $F : \mathcal{A} \times \mathcal{A} \to \mathbb{C}$ where for $\boldsymbol{a} \in \mathcal{A}, \boldsymbol{b} \in \mathcal{A}$,

$$F(\boldsymbol{a}, \boldsymbol{b}) = 1 + <-\boldsymbol{a}, \boldsymbol{b}> + <-\boldsymbol{a}, 2\boldsymbol{b}> + <-\boldsymbol{a}, \boldsymbol{b}><-\boldsymbol{a}, 2\boldsymbol{b}>.$$

Lemma 10. *For any $\boldsymbol{a}, \boldsymbol{b} \in \mathcal{A}$,*

$$F(\boldsymbol{a}, \boldsymbol{b}) = \begin{cases} 4 & \text{if } \boldsymbol{a}^T \cdot \boldsymbol{b} = \sum_{i=1}^{r} a_i b_i \equiv 0 \mod 3, \text{ and} \\ 1 & \text{otherwise.} \end{cases}$$

Proof: First consider the case where $\boldsymbol{a}^T \cdot \boldsymbol{b} \equiv 0 \mod 3$. Notice that if $\boldsymbol{a}^T \cdot \boldsymbol{b} \equiv 0 \mod 3$, then $<\boldsymbol{a}, \boldsymbol{b}> = 1$. Since $\boldsymbol{a}^T \cdot \boldsymbol{b} \equiv 0 \mod 3$ we have $-\boldsymbol{a}^T \cdot \boldsymbol{b} = -\boldsymbol{a}^T \cdot 2\boldsymbol{b} \equiv 0 \mod 3$ and so the quantity in the Lemma is equal to 4.

Consider the case now where $\boldsymbol{a}^T \cdot \boldsymbol{b} \not\equiv 0 \mod 3$. Recall ζ_3 is a cubic root of unity and note that $<-\boldsymbol{a}, 2\boldsymbol{b}> = <-\boldsymbol{a}, \boldsymbol{b}>^2$. Then,

$$\begin{aligned} &<-\boldsymbol{a}, \boldsymbol{b}> + <-\boldsymbol{a}, 2\boldsymbol{b}> + <-\boldsymbol{a}, \boldsymbol{b}><-\boldsymbol{a}, 2\boldsymbol{b}> \\ &= <-\boldsymbol{a}, \boldsymbol{b}> + <-\boldsymbol{a}, \boldsymbol{b}>^2 + <-\boldsymbol{a}, \boldsymbol{b}>^3 \\ &= \zeta_3 + \zeta_3^2 + \zeta_3^3 \\ &= 0, \end{aligned}$$

and so $F(\boldsymbol{a}, \boldsymbol{b}) = 1$. ∎

Given an input $\boldsymbol{c} \in \mathcal{A}$, let $\beta : \mathcal{A} \to \{0, \ldots, \ell\}$ be defined as follows

$$\beta(\boldsymbol{c}) = |\{1 \leq i \leq \ell : \boldsymbol{c}^T \cdot \boldsymbol{h}'_i \equiv 0 \mod 3\}| \tag{14}$$

where $\boldsymbol{h}'_i$ refers to the i-th column of H'.

The following function will be used in the proof of Theorem 5. Let $I : GF(2)^{2\ell} \times \mathcal{A} \to \{0, 1\}$ denote the indicator function where for $\boldsymbol{x} \in GF(2)^{2\ell}$ and $\boldsymbol{a} \in \mathcal{A}$,

$$I(\boldsymbol{x}, \boldsymbol{a}) = \begin{cases} 1 & \text{if } \gamma(\boldsymbol{x}) = \boldsymbol{a}, \\ 0 & \text{otherwise} \end{cases} \tag{15}$$

where γ is as defined in (12).

We are now ready for the main result of this section.

Theorem 5. *For any $\boldsymbol{b} \in \mathcal{A}$, $f(\boldsymbol{b}) = \frac{1}{3^r} \sum_{\boldsymbol{a} \in \mathcal{A}} <\boldsymbol{b}, \boldsymbol{a}> 4^{\beta(\boldsymbol{a})}$.*

Proof: Consider $\boldsymbol{c} \in \mathcal{A}$. As in [11], we proceed by computing the Fourier transform $\hat{f}(\boldsymbol{c})$ (as defined as in Section II-E). First note that from (15), we can write $f(\boldsymbol{a}) = \sum_{\boldsymbol{x} \in GF(2)^{2\ell}} I(\boldsymbol{x}, \boldsymbol{a})$ where $\boldsymbol{a} \in \mathcal{A}$. We have

$$\begin{aligned} \hat{f}(\boldsymbol{c}) &= \sum_{\boldsymbol{a} \in \mathcal{A}} <\boldsymbol{c}, -\boldsymbol{a}> f(\boldsymbol{a}) \\ &= \sum_{\boldsymbol{a} \in \mathcal{A}} <-\boldsymbol{c}, \boldsymbol{a}> f(\boldsymbol{a}) \\ &= \sum_{\boldsymbol{a} \in \mathcal{A}} <-\boldsymbol{c}, \boldsymbol{a}> \sum_{x \in GF(2)^{2\ell}} I(\boldsymbol{x}, \boldsymbol{a}) \\ &= \sum_{\boldsymbol{a} \in \mathcal{A}} \sum_{\boldsymbol{x} \in GF(2)^{2\ell}} <-\boldsymbol{c}, \boldsymbol{a}> I(\boldsymbol{x}, \boldsymbol{a}) \\ &= \sum_{\boldsymbol{x} \in GF(2)^{2\ell}} \sum_{\boldsymbol{a} \in \mathcal{A}} <-\boldsymbol{c}, \boldsymbol{a}> I(\boldsymbol{x}, \boldsymbol{a}). \end{aligned}$$

Note that for a fixed $\boldsymbol{x} \in GF(2)^{2\ell}$, $\sum_{\boldsymbol{a} \in \mathcal{A}} <-\boldsymbol{c}, \boldsymbol{a}> I(\boldsymbol{x}, \boldsymbol{a}) = <-\boldsymbol{c}, \gamma(\boldsymbol{x})>$. Then,

$$\begin{aligned} \hat{f}(\boldsymbol{c}) &= \sum_{\boldsymbol{x} \in GF(2)^{2\ell}} <-\boldsymbol{c}, \gamma(\boldsymbol{x})> \\ &= \sum_{\boldsymbol{x} \in GF(2)^{2\ell}} <-\boldsymbol{c}, x_1 \boldsymbol{h}_1 + \cdots + x_{2\ell} \boldsymbol{h}_{2\ell}> \\ &= \sum_{\boldsymbol{x} \in GF(2)^{2\ell}} <-\boldsymbol{c}, x_1 \boldsymbol{h}_1> \cdots <-\boldsymbol{c}, x_{2\ell} \boldsymbol{h}_{2\ell}>, \end{aligned}$$

where the last equality follows from the property that for $\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3 \in \mathcal{A}$, $<-\boldsymbol{a}_1, \boldsymbol{a}_2 + \boldsymbol{a}_3> = <-\boldsymbol{a}_1, \boldsymbol{a}_2><-\boldsymbol{a}_1, \boldsymbol{a}_3>$.

Notice that each x_i is equal to either 0 or 1 (where $1 \leq i \leq 2\ell$). If $x_i = 0$, then clearly $<-\boldsymbol{c}, x_i \boldsymbol{h}_i> = 1$. If $x_i = 1$, $<-\boldsymbol{c}, x_i \boldsymbol{h}_i> = <-\boldsymbol{c}, \boldsymbol{h}_i>$. Thus, by suitably collecting terms (and by induction on ℓ), we can write

$$\hat{f}(\boldsymbol{c}) = \prod_{i=1}^{2\ell} (1 + <-\boldsymbol{c}, \boldsymbol{h}_i>).$$

Let j be an integer such that $1 \leq j \leq \ell$. Then from the definition of H (see also (12)) we can write $(1 + <-\boldsymbol{c}, \boldsymbol{h}_{2j}>)(1 + <-\boldsymbol{c}, \boldsymbol{h}_{2j-1}>) = (1 + <-\boldsymbol{c}, \boldsymbol{h}'_j>)(1 + <-\boldsymbol{c}, 2\boldsymbol{h}'_j>)$. Thus, we can rewrite $\hat{f}(\boldsymbol{c})$ in terms of the $\boldsymbol{h}'_i$ terms so that

$$\begin{aligned} \hat{f}(\boldsymbol{c}) &= \prod_{i=1}^{\ell} (1 + <-\boldsymbol{c}, \boldsymbol{h}'_i> + <-\boldsymbol{c}, 2\boldsymbol{h}'_i> + \\ &\qquad <-\boldsymbol{c}, \boldsymbol{h}'_i><-\boldsymbol{c}, 2\boldsymbol{h}'_i>) \\ &= \prod_{i=1}^{\ell} F(\boldsymbol{c}, \boldsymbol{h}'_i) \\ &= 4^{\beta(\boldsymbol{c})}. \end{aligned}$$

The equality follows from Lemma 10. Recall, from Section II-E that the inverse Fourier transform of $\hat{f}$ is $f(\boldsymbol{b}) =$

TABLE III
COMPARISON OF SIZES OF GRAIN-ERROR-CORRECTING CODES WITH THE LOWER BOUND FROM COROLLARY 7

Length	$t=2$	$t=3$	$t=4$
11	68/32	-	-
13	132/44	-	-
15	312/146	260/62	-
17	836/550	516/84	-
19	2636/2168	1028/114	1028/114
21	9376/8640	2144/354	2052/154
23	35648/34532	4688/1312	4100/208
25	49024/46044	8896/1752	8320/634
27	190912/184128	20808/6866	17216/2338
29	747520/736464	41616/27324	34096/3120

$\frac{1}{3^r}\sum_{\boldsymbol{a}\in\mathcal{A}} <\boldsymbol{a},\boldsymbol{b}>\hat{f}(\boldsymbol{a})$. Thus, since $\hat{f}(\boldsymbol{a}) = 4^{\beta(\boldsymbol{a})}$, we have that for an element $\boldsymbol{b}\in\mathcal{A}$,

$$\begin{aligned} f(\boldsymbol{b}) &= \frac{1}{3^r}\sum_{\boldsymbol{a}\in\mathcal{A}} <\boldsymbol{a},\boldsymbol{b}>\hat{f}(\boldsymbol{a}) \\ &= \frac{1}{3^r}\sum_{\boldsymbol{a}\in\mathcal{A}} <\boldsymbol{a},\boldsymbol{b}>4^{\beta(\boldsymbol{a})}. \end{aligned}$$

■

Corollary 6. *For any $\boldsymbol{b}\in\mathcal{A}$, $f(\boldsymbol{b})\le f(\boldsymbol{0})$.*

Proof: As in [11], this is because for any $\boldsymbol{a},\boldsymbol{b}\in\mathcal{A}$, $|<\boldsymbol{a},\boldsymbol{b}>| \le 1$. Thus, $f(\boldsymbol{b}) = \frac{1}{3^r}\sum_{\boldsymbol{a}\in\mathcal{A}} <\boldsymbol{b},\boldsymbol{a}>4^{\beta(\boldsymbol{a})} \le \frac{1}{3^r}\sum_{\boldsymbol{a}\in\mathcal{A}} 4^{\beta(\boldsymbol{a})} = f(\boldsymbol{0})$. ■

Thus, choosing $\boldsymbol{a}=\boldsymbol{0}$ in Construction C maximizes the cardinality of the resulting code. The following lemma is another consequence of Theorem 5.

Lemma 11. *For positive integers r,ℓ where $r<\ell$, $f(\boldsymbol{0}) \ge \frac{4^\ell}{3^r} + 2\left(\frac{4}{3}\right)^r - 2\cdot\frac{4}{3}$.*

Proof: From Theorem 5, we have that $f(\boldsymbol{0}) = \frac{1}{3^r}\sum_{\boldsymbol{a}\in\mathcal{A}} 4^{\beta(\boldsymbol{a})}$. Clearly, $\beta(\boldsymbol{0}) = \ell$ and so $f(\boldsymbol{0}) = \frac{1}{3^r}\left(4^\ell + \sum_{\boldsymbol{a}\in\mathcal{A},\boldsymbol{a}\neq\boldsymbol{0}} 4^{\beta(\boldsymbol{a})}\right)$. We define the sets $\mathcal{T}_0 = \{\boldsymbol{0}\}, \mathcal{N}_0 = \{\boldsymbol{0}\}$, and $\mathcal{N}'_0 = \{\boldsymbol{0}\}$.

In the following we define the sets $\mathcal{N}_j, \mathcal{N}'_j$, and $\mathcal{T}_j$ recursively (starting at $j=1$) where j is an integer such that $1\le j\le r-1$. Consider the sub-matrix H'_j consisting of the first $r-j$ columns of H' where H' is the parity check matrix for $\mathcal{C}'$ with columns h'_i and $1\le i\le \ell$. Let $\mathcal{N}_j = \{\boldsymbol{g}\in\mathcal{A} : \boldsymbol{g}^T\cdot H'_j = \boldsymbol{0}\}$. Notice that since H'_j has rank at most $r-j$, $|\mathcal{N}_j|\ge 3^j$. Let $\mathcal{N}'_j\subseteq\mathcal{N}_j$ be such that $|\mathcal{N}'_j| = 3^j$. We briefly note that the elements in $\mathcal{N}'_j$ can be chosen arbitrarily from $\mathcal{N}_j$. Let $\mathcal{T}_j = \mathcal{N}'_j\setminus\mathcal{N}'_{j-1}$. Under this setup, for any $0\le k<j$, $\mathcal{T}_j\cap\mathcal{T}_k=\emptyset$. Now, for any $\mathcal{T}_j$, we have

$$|\mathcal{T}_j| = |\mathcal{N}'_j| - |\mathcal{N}'_{j-1}| = 3^j - 3^{j-1}.$$

Notice that for any $\boldsymbol{u}\in\mathcal{T}_j$, $\beta(\boldsymbol{u}) = |\{1\le i\le\ell : \boldsymbol{u}^T\cdot \boldsymbol{h}'_i = \boldsymbol{0}\}| \ge r-j$. Then since the sets $\mathcal{T}_0,\mathcal{T}_1,\ldots,\mathcal{T}_{r-1}$ are non-overlapping (they have no common elements), we can use Theorem 5 with $\boldsymbol{b}=\boldsymbol{0}$ to obtain $f(\boldsymbol{0}) = \frac{1}{3^r}\sum_{\boldsymbol{a}\in\mathcal{A}} 4^{\beta(\boldsymbol{a})} \ge \frac{1}{3^r}|\mathcal{T}_0|4^\ell + \frac{1}{3^r}\sum_{j=1}^{r-1}|\mathcal{T}_j|4^{r-j}$. Finally,

$$\begin{aligned} f(\boldsymbol{0}) &\ge \frac{1}{3^r}|\mathcal{T}_0|4^\ell + \frac{1}{3^r}\sum_{j=1}^{r-1}|\mathcal{T}_j|4^{r-j} \\ &\ge \frac{1}{3^r}4^\ell + \frac{1}{3^r}\sum_{j=1}^{r-1}(3^j-3^{j-1})4^{r-j} \\ &= \frac{1}{3^r}4^\ell + \frac{2\cdot 4^{r-1}}{3^r}\sum_{j=0}^{r-2}\left(\frac{3}{4}\right)^j \\ &= \frac{1}{3^r}4^\ell + 2\left(\frac{4}{3}\right)^r - 2\cdot\frac{4}{3}, \end{aligned}$$

and therefore the proof is complete. ■

We summarize the result from Lemma 11 with the following corollary.

Corollary 7. *Let $\mathcal{C}'$ be a t-random-error-correcting ternary code of length $\ell = \frac{n}{2}$ (where n is an even integer) with a parity check matrix H' of dimension r. For $\boldsymbol{a}\in\mathcal{A}$, let $\mathcal{C}_{\boldsymbol{a}}$ be a code created according to Construction C of length n with the constituent code $\mathcal{C}'$. Then for any $\boldsymbol{a}\in\mathcal{A}$, $|\mathcal{C}_{\boldsymbol{a}}|\le|\mathcal{C}_{\boldsymbol{0}}|$ and $|\mathcal{C}_{\boldsymbol{0}}| \ge \frac{2^n}{3^r} + 2\left(\frac{4}{3}\right)^r - \frac{8}{3}$.*

Proof: From Claim 7, $|\mathcal{C}_a| = f(\boldsymbol{a})$. Using Corollary 6, we have that for any $\boldsymbol{a}\in\mathcal{A}$, $|\mathcal{C}_{\boldsymbol{a}}| = f(\boldsymbol{a}) \le f(\boldsymbol{0}) = |\mathcal{C}_{\boldsymbol{0}}|$. Combining Claim 7 and Lemma 11 gives that $|\mathcal{C}_{\boldsymbol{0}}| = f(\boldsymbol{0}) \ge \frac{4^\ell}{3^r} + 2\left(\frac{4}{3}\right)^r - 2\cdot\frac{4}{3}$. ■

Thus, the previous corollary improved upon Corollary 5 where it was shown that for some $\boldsymbol{a}\in\mathcal{A}$, $|\mathcal{C}_{\boldsymbol{a}}|\ge\frac{2^n}{3^r}$. For the case of $t=2,3,4$, we compared our lower bound with the cardinality of the t-grain-error-correcting codes from Table II. Each entry in Table III contains two numbers delimited by a '/'. The first number is the cardinality of a t-grain-error-correcting code created according to Construction B (from Table II) and the second number is the lower bound from Corollary 7. It can be seen in Table III that the difference between the bound from Corollary 7 and the size of the codes from Table II is small for the $t=2$ case.

In the next section, we return to the problem of constructing single mineral codes.

VI. General Single-Grain and Single-Mineral Codes from Construction B

In this Section, we consider single-mineral codes derived from more general colorings according to Construction B. In Section VI-A, we investigate a sufficient condition for codes created with Construction B to produce large single-mineral codes. In Section VI-B, we consider the cardinalities of codes created according to Construction B given a coloring based on the group codes [2]. In Section VI-C, we describe a coloring that was found using a computerized search, and for code lengths 48 and 342 this coloring produces new codes with large cardinalities (larger than using the alternative group codes to construct single mineral-codes).

Recall from Construction B in Section IV-B that the construction for a t-mineral-error-correcting code $\mathcal{C}$ relied on two key ingredients:

1) a mapping $\Phi_{t,m}$ from $GF(2)^m$ to p color classes (where p is a prime), and
2) a t-random-error-correcting code $\mathcal{C}_t$ over $GF(p)$.

The basic idea behind Construction B was to use $\Phi_{t,m}$ to map the color classes of a p-coloring onto the symbols of the non-binary code $\mathcal{C}_t$.

Thus far, we have considered code constructions for mineral codes using Construction B with the map $\Phi_{t,m} = \Gamma$, where Γ is given by (7). Therefore, if Construction B is used to create mineral codes, there are two possible directions to investigate:

1) discover new mappings $\Phi_{t,m}$ for $m \geq 2$, and
2) investigate codes for $\mathcal{C}_t$ that, when used in conjunction with some $\Phi_{t,m}$, result in codes with large cardinalities.

In this section, we focus on the first direction for the case where $t = 1$, where the code $\mathcal{C}_1$ is a single random-error-correcting code that is a Hamming code. The second item highlights a potential area of future work which we will discuss briefly in the next section.

In the first subsection, we show that if $\Phi_{t,m}$ has $p = m+1$ color classes where p is a prime, then it is possible to construct single-mineral codes that have at least as many codewords as perfect single random-error-correcting binary codes of the same length. In the second subsection, single-mineral codes created using a coloring scheme based upon the group codes are considered. Motivated by the insights from the first two subsections, we derive new codes of lengths 48 and 342 in the third subsection. These new codes are larger than any codes of the same length produced according to Construction A.

A. A sufficient condition for Construction B to produce large codes

Suppose that a single-mineral code $\mathcal{C}$ of length mn is created according to Construction B. Suppose that the p-coloring $\Phi_{1,m}$ is such that $p = m + 1$ where p is an odd prime and $\mathcal{C}_1$ is a perfect non-binary single random-error-correcting code over $GF(p)$ of length n. We show that there exists a mineral code $\mathcal{C}$ of length mn whose cardinality is at least $\frac{2^{mn}}{mn+1}$. Motivated by this observation, in Sections VI-B and VI-C, we consider using different coloring schemes (i.e., where $\Phi_{1,m} \neq \Gamma$) in conjunction with a perfect single-random-error correcting code. We first begin by reviewing some notation that was used in Section IV-B.

As in Section IV-B, let $\mathcal{G}_{t,m} = (V, E)$ denote a simple graph where $V = GF(2)^m$, and for any $\boldsymbol{x}, \boldsymbol{y} \in V$ (where $\boldsymbol{x} \neq \boldsymbol{y}$) $(\boldsymbol{x}, \boldsymbol{y}) \in E$ if $\mathcal{B}_{t,M}(\boldsymbol{x}) \cap \mathcal{B}_{t,M}(\boldsymbol{y}) \neq \emptyset$. Recall that $\Phi_{t,m} : GF(2)^m \to GF(p)$ is a p-coloring if it assigns different elements of $GF(p)$ to adjacent vertices. From Section II-C, $\chi(\mathcal{G}_{t,m})$ is the smallest p for which a p-coloring is possible. Recall, the size of the largest clique in a graph $\mathcal{G}$ is denoted $\varsigma(\mathcal{G})$.

The following claim will be used in the proof of Lemma 12.

Claim 8. *For any $m \geq 2$, $\varsigma(\mathcal{G}_{1,m}) \geq m + 1$.*

Proof: Let $\mathcal{S} = \{\boldsymbol{x} \in GF(2)^m : wt(\boldsymbol{x}) \leq 1\}$. Since for any $\boldsymbol{x} \in \mathcal{S}$, $\mathcal{B}_{1,m}(\boldsymbol{x})$ contains the all-zeros vector, it follows that $\mathcal{S}$ is a clique in $\mathcal{G}_{1,m}$. Since $|\mathcal{S}| = m + 1$, the result follows. ■

Lemma 12. *Let m be a positive integer. Then, $\chi(\mathcal{G}_{1,m}) = m + 1$.*

Proof: We first show that $\chi(\mathcal{G}_{1,m}) \leq m+1$. Suppose $\mathcal{A}$ is an Abelian group. Let $a \in \mathcal{A}$ and consider a single-grain code $\mathcal{C}_a^{\mathcal{A}}$ of length $|\mathcal{A}| = m + 1$ created using Construction A. Let $\tilde{\mathcal{C}}_a^{\mathcal{A}}$ be the group code of length m that is the result of shortening the codewords in $\mathcal{C}_a^{\mathcal{A}}$ on the first bit. From Corollary 2, $\tilde{\mathcal{C}}_a^{\mathcal{A}}$ is a single-mineral code. Assign to every $\boldsymbol{x} \in \tilde{\mathcal{C}}_a^{\mathcal{A}}$ the same number from $\{0, 1, \ldots, m\}$. Repeating this process for every value of $a \in \mathcal{A}$ (and using a different number for different values of a), results in an $(m + 1)$-coloring on the graph $\chi(\mathcal{G}_{1,m})$ since there are $|\mathcal{A}| = m+1$ choices for a.

Recall from Section II-C that $\chi(\mathcal{G}_{1,m}) \geq \varsigma(\mathcal{G}_{1.m})$ where $\varsigma(\mathcal{G}_{1,m})$ is the maximum size of any clique in the graph $\mathcal{G}_{1,m}$. From Claim 8, we have $\chi(\mathcal{G}_{1,m}) \geq \varsigma(\mathcal{G}_{1,m}) \geq m + 1$ and so $\chi(\mathcal{G}_{1,m}) = m + 1$. ■

The following theorem is similar to Corollary 5.

Theorem 6. *Let p be a prime number and r a positive integer where $n = \frac{p^r-1}{p-1}$ and $m = p - 1$. Then there exists a single-mineral code $\mathcal{C}$ of length mn where $|\mathcal{C}| \geq \frac{2^{mn}}{mn+1}$ from Construction B.*

Proof: Let $\mathcal{C}_1$ be the constituent non-binary code from Construction B of length n with a parity check matrix H' of dimension r and suppose that $\mathcal{C}_1$ is perfect and $\mathcal{A} = GF(p)^r$. For $\boldsymbol{a} \in \mathcal{A}$, let $\mathcal{C}'_{\boldsymbol{a}} = \{\boldsymbol{x}' \in GF(p)^n : H' \cdot \boldsymbol{x}' = \boldsymbol{a}\}$. Notice that since $\mathcal{C}_1$ is a perfect single random-error-correcting code then $\mathcal{C}'_{\boldsymbol{a}}$ is also a perfect single random-error-correcting code. Thus, we can apply Construction B to obtain a single-mineral code $\mathcal{C}_{\boldsymbol{a}}$ where

$$\mathcal{C}_{\boldsymbol{a}} = \{\boldsymbol{x} \in GF(2)^{mn} : \Phi_{1,m}(\boldsymbol{x}) \in \mathcal{C}'_{\boldsymbol{a}}\}.$$

Since $\Phi_{1,m}$ maps every element in $GF(2)^{mn}$ to exactly one non-binary vector of length n, it follows that every

$\boldsymbol{x} \in GF(2)^{mn}$ belongs to exactly one $\mathcal{C}_{\boldsymbol{a}}$, and so the codes $\mathcal{C}_{\boldsymbol{a}_1}, \mathcal{C}_{\boldsymbol{a}_2}, \ldots, \mathcal{C}_{\boldsymbol{a}_{p^r}}$ partition the space $GF(2)^{mn}$ into p^r non-overlapping sets. By the pigeonhole principle, there exists a $\boldsymbol{b} \in \mathcal{A}$, where $|\mathcal{C}_{\boldsymbol{b}}| \geq \frac{2^{mn}}{p^r} = \frac{2^{mn}}{mn+1}$. ■

We now consider using the coloring scheme discussed in the proof of Lemma 12 to produce single-mineral codes. More precisely, let $\psi_m : GF(2)^m \to GF(m+1)$ be the mapping so that for a vector $\boldsymbol{x} \in GF(2)^m$,

$$\psi_m(\boldsymbol{x}) = \sum_{i=1}^{m} i x_i \mod m+1.$$

Then, let $A_j = \{\boldsymbol{y} \in GF(2)^m : \psi_m(\boldsymbol{y}) = j\}$. We refer to the vector $(A_0, A_1, \ldots, A_m)$ as the ***group-code partition***. Let Π_m be the set of permutations of the symbols $0, 1, \ldots, m$. For example, the permutation $(1, 0, 2)$ is an element in Π_2. Then, for any permutation $\boldsymbol{a} = (a_0, \ldots, a_m) \in \Pi_m$, we define a coloring $\Phi_{\boldsymbol{a}} : GF(2)^m \to GF(m+1)$ as follows

$$\Phi_{\boldsymbol{a}}(\boldsymbol{x}) = a_{\psi_m(\boldsymbol{x})}.$$

We provide an example illustrating this mapping.

Example 5. *Let $\boldsymbol{a} = (1, 0, 2)$ so that $m = 2$. Let $\boldsymbol{x}_1 = (1, 1)$ so that $\Phi_{\boldsymbol{a}}(\boldsymbol{x}_1) = a_{\psi_2(\boldsymbol{x}_1)} = a_0 = 1$. Similarly for $\boldsymbol{x}_2 = (0, 1)$, we have $\Phi_{\boldsymbol{a}}(\boldsymbol{x}_2) = a_{\psi_2(\boldsymbol{x}_2)} = a_2 = 2$.*

Suppose the single-mineral code $\mathcal{C}$ is constructed according to Construction B with $\Phi_{\boldsymbol{a}}$ and the single random-error-correcting non-binary code $\mathcal{C}_1$ with symbols over $GF(m+1)$. For shorthand, we refer to $\mathcal{C}$ as $\mathcal{C}(\boldsymbol{a}, \mathcal{C}_1)$.

In the next subsection, we determine which choice of $\boldsymbol{a}$ maximizes the cardinality $|\mathcal{C}(\boldsymbol{a}, \mathcal{C}_1)|$ when $\mathcal{C}_1$ is a linear code. In Section VI-C a different map $\Phi_{1,6}$ is derived using a computerized search over the space $GF(2)^6$ and using this map better single-mineral codes are found for certain code lengths.

B. Single-mineral codes created using the group-code partition

In this section, we consider the problem of which choice of $\boldsymbol{a} \in \Pi_m$ maximizes $|\mathcal{C}(\boldsymbol{a}, \mathcal{C}_1)|$ when $\mathcal{C}_1$ is a linear code. We show that any $\boldsymbol{a} = (a_0, \ldots, a_m) \in \Pi_m$ where $a_0 = 0$ maximizes the cardinality of the resulting single-mineral code. Since the largest color class under ψ_m is A_0 (cf. [2]), one such choice for $\boldsymbol{a}$ is the identity (i.e., $\boldsymbol{a} = (0, 1, 2 \ldots, m)$). For shorthand, let $\boldsymbol{i} = (0, 1, 2, \ldots, m)$. We show that the cardinality of $\mathcal{C}(\boldsymbol{i}, \mathcal{C}_1)$ is exactly the same as the cardinality of a code created according to the Constantin-Rao construction (for codes of the same length) [2].

For a non-binary code $\mathcal{C}$ with symbols from $GF(p)$ where p is an odd prime, let $W_{i_0,\ldots,i_{p-1}}$ denote the number of codewords in $\mathcal{C}$ that have exactly i_0 symbols of value 0, i_1 symbols of value 1, and so on. We denote the ***complete weight enumerator*** of $\mathcal{C}$ as

$$W_{\mathcal{C}}(z_0, \ldots, z_{p-1}) = \sum_{i_0, i_1, \ldots, i_{p-1}} W_{i_0,\ldots,i_{p-1}} z_0^{i_0} \cdots z_{p-1}^{i_{p-1}}.$$

We make use of the following known claim [6] [13] in Theorem 7, which can be proven using the MacWilliams Theorem (see Appendix B). Recall ζ_p is a p-th root of unity and p is a prime. For an integer i, ζ_p^i denotes the i-th power of ζ_p.

Claim 9. *(c.f. [6],[13]) Suppose $\mathcal{C}$ is a linear code of length n with symbols over $GF(p)$. Then, the complete weight enumerator $W_{\mathcal{C}}(z_0, \ldots, z_{p-1})$ can be written in terms of the codewords in the dual code $\mathcal{C}^\perp$ (of $\mathcal{C}$) as follows*

$$\frac{1}{|\mathcal{C}^\perp|} \sum_{\boldsymbol{c}=(c_1,\ldots,c_n)\in\mathcal{C}^\perp} \prod_{i=1}^{n} \left(z_0 + z_1 \zeta_p^{1\cdot c_i} + \ldots + z_{p-1} \zeta_p^{(p-1)\cdot c_i} \right).$$

The next claim will also be useful in the proof of Theorem 7.

Claim 10. *Let j^*, c be integers such that $0 \leq j^* \leq p-1$ and $c \neq 0$. Then, $\sum_{j=0, j\neq j^*}^{p-1} \zeta_p^{j\cdot c} = -\zeta_p^{j^*\cdot c}$.*

We make use of the following notation in the statement of the next claim. For any $\boldsymbol{a} \in \Pi_m$ (recall Π_m is the set of permutations of the symbols $0, 1, \ldots, m$) and any integer k where $0 \leq k \leq m$ let $\boldsymbol{a}(k)$ denote the index in $\boldsymbol{a}$ of the number k.

Claim 11. *Let $m+1$ be an odd prime. Suppose $W_{\mathcal{C}_1}(z_0, \ldots, z_m)$ is the complete weight enumerator for a non-binary $(m+1)$-ary code $\mathcal{C}_1$. Then for any $\boldsymbol{a} \in \Pi_m$, $|\mathcal{C}(\boldsymbol{a}, \mathcal{C}_1)| = W_{\mathcal{C}_1}(|A_{\boldsymbol{a}(0)}|, \ldots, |A_{\boldsymbol{a}(m)}|)$.*

We are now ready to state the main result of this subsection.

Theorem 7. *Suppose $\mathcal{C}_1$ is a linear code over $GF(m+1)$ where $m+1$ is an odd prime. For any $\boldsymbol{a} \in \Pi_m$, $|\mathcal{C}(\boldsymbol{a}, \mathcal{C}_1)|$ is maximized when $a_0 = 0$. Furthermore for any $\boldsymbol{b} \in \Pi_m$ where $b_0 = 0$, $|\mathcal{C}(\boldsymbol{a}, \mathcal{C}_1)| = |\mathcal{C}(\boldsymbol{b}, \mathcal{C}_1)|$.*

Proof: Let $p = m+1$ and $\boldsymbol{a} = (a_0, \ldots, a_m)$. Under the group-code partition, the largest color class A_0 has cardinality $\frac{2^{p-1}+p-1}{p}$ and the other color classes have cardinality $\frac{2^{p-1}-1}{p}$ ([2]). We prove the theorem by considering the cardinality of the code created according to Construction B when the color classes from the group-code partition are mapped to different symbols in $GF(p)$. From Claim 11, the cardinality of the mineral code $\mathcal{C}(\boldsymbol{a}, \mathcal{C}_1)$ created according to Construction B can be derived from $W_{\mathcal{C}_1}(z_0, \ldots, z_{p-1})$ by substituting for each z_i, the size of the color class that is mapped to symbol i (as a result of the permutation $\boldsymbol{a}$). Suppose $\mathcal{C}_1^\perp$ represents the dual code of $\mathcal{C}_1$. Then, from Claims 9 and 11, we can write $|\mathcal{C}(\boldsymbol{a}, \mathcal{C}_1)| = \frac{1}{|\mathcal{C}_1^\perp|} \sum_{\boldsymbol{c}\in\mathcal{C}_1^\perp} \prod_{i=1}^{n} (|A_{\boldsymbol{a}(0)}| + |A_{\boldsymbol{a}(1)}| \zeta_p^{1\cdot c_i} + \ldots + |A_{\boldsymbol{a}(p-1)}| \zeta_p^{(p-1)\cdot c_i})$.

In particular, we consider the term

$$\Lambda(\boldsymbol{a}, c_i) = \left(|A_{\boldsymbol{a}(0)}| + |A_{\boldsymbol{a}(1)}| \zeta_p^{1\cdot c_i} + \ldots + |A_{\boldsymbol{a}(p)}| \zeta_p^{(p-1)\cdot c_i} \right) \tag{16}$$

for certain choices of $\boldsymbol{a}$ and $c_i \in GF(p)$. Note that under this setup $|\mathcal{C}(\boldsymbol{a}, \mathcal{C}_1)| = \frac{1}{|\mathcal{C}_1^\perp|} \sum_{\boldsymbol{c}\in\mathcal{C}_1^\perp} \prod_{i=1}^{n} \Lambda(\boldsymbol{a}, c_i)$.

We consider two cases:

1) $a_0 = 0$, or
2) $a_0 \neq 0$.

In the remainder of the proof we refer to the setup in item 1) above as Case 1) and the setup in item 2) above as Case 2). Notice that under either Case 1) or Case 2), we have $\Lambda(\boldsymbol{a}, 0) = \sum_{k=0}^{p-1} |A_{\boldsymbol{a}(k)}| = 2^{p-1}$. In the following two cases, we therefore only consider the quantity $\Lambda(\boldsymbol{a}, c)$ where $c \in GF(p)$ and $c \neq 0$.

Case 1: Suppose $\boldsymbol{a}$ is such that $a_0 = 0$. Then $\Lambda(\boldsymbol{a}, c_i)$ (where $c_i \neq 0, c_i \in GF(p)$) can be written as

$$\Lambda(\boldsymbol{a}, c_i) = \frac{2^{p-1} + p - 1}{p} + \frac{2^{p-1} - 1}{p} \sum_{k=1}^{p-1} \zeta_p^{k \cdot c_i}.$$

Applying Claim 10, we get that $\Lambda(\boldsymbol{a}, c_i) = 1$ when $c_i \neq 0$.

Case 2: Suppose $\boldsymbol{a}$ is such that $a_0 \neq 0$. In particular, we assume $a_{j^*} = 0$ for $j^* \neq 0$. Then, we can write $\Lambda(\boldsymbol{a}, c_i)$ as (where $c_i \neq 0, c_i \in GF(p)$)

$$\begin{aligned}\Lambda(\boldsymbol{a}, c_i) &= \frac{2^{p-1} + p - 1}{p} \zeta_p^{j^* c_i} + \frac{2^{p-1} - 1}{p} \sum_{j=0, j \neq j^*}^{p-1} \zeta_p^{j c_i} \\ &= \frac{2^{p-1} + p - 1}{p} \zeta_p^{j^* c_i} + \frac{2^{p-1} - 1}{p} \left(-\zeta_p^{j^* c_i} \right) \\ &= \zeta_p^{j^* c_i}.\end{aligned}$$

Notice that $|\zeta_p^{j^* c_i}| \leq 1$ for any integer $j^* \neq 0$.

Summary: Using the ideas from above, we now show that $\mathcal{C}(\boldsymbol{a}, \mathcal{C}_1)$ is maximized when $a_0 = 0$. Consider any $\boldsymbol{b} = (b_0, b_1, \ldots, b_m), \boldsymbol{d} = (d_0, d_1, \ldots, d_m) \in \Pi_m$ where $b_0 = 0 \neq d_0$. From the previous analysis, for any $c_i \in GF(p)$ we have $|\Lambda(\boldsymbol{d}, c_i)| \leq \Lambda(\boldsymbol{b}, c_i)$ and so

$$\frac{1}{|\mathcal{C}_1^\perp|} \sum_{\boldsymbol{c} \in \mathcal{C}_1^\perp} \prod_{i=1}^{n} \Lambda(\boldsymbol{d}, c_i) \leq \frac{1}{|\mathcal{C}_1^\perp|} \sum_{\boldsymbol{c} \in \mathcal{C}_1^\perp} \prod_{i=1}^{n} \Lambda(\boldsymbol{b}, c_i),$$

and

$$|\mathcal{C}(\boldsymbol{d}, \mathcal{C}_1)| \leq |\mathcal{C}(\boldsymbol{b}, \mathcal{C}_1)|.$$

Let $\boldsymbol{g} = (g_0, g_1, \ldots, g_m) \in \Pi_m$ where $g_0 = 0$ but $\boldsymbol{g} \neq \boldsymbol{b}$. We have left to show that for any such $\boldsymbol{g}$, $|\mathcal{C}(\boldsymbol{g}, \mathcal{C}_1)| = |\mathcal{C}(\boldsymbol{b}, \mathcal{C}_1)|$ where $\boldsymbol{b}$ is as defined in the previous paragraph. From the previous analysis, for any $c_i \in GF(p)$ we have $\Lambda(\boldsymbol{d}, c_i) = \Lambda(\boldsymbol{b}, c_i)$ and so $|\mathcal{C}(\boldsymbol{d}, \mathcal{C}_1)| = \frac{1}{|\mathcal{C}_1^\perp|} \sum_{\boldsymbol{c} \in \mathcal{C}_1^\perp} \prod_{i=1}^{n} \Lambda(\boldsymbol{d}, c_i) = \frac{1}{|\mathcal{C}_1^\perp|} \sum_{\boldsymbol{c} \in \mathcal{C}_1^\perp} \prod_{i=1}^{n} \Lambda(\boldsymbol{b}, c_i) = |\mathcal{C}(\boldsymbol{b}, \mathcal{C}_1)|$. ■

From Theorem 7, to maximize the size of a mineral code $\mathcal{C}$ created according to Construction B with a group-code partition, the largest color class A_0 should be mapped to the symbol zero in the constituent code $\mathcal{C}_1$. Suppose the Hamming weight enumerator of a code $\mathcal{C}$ can be written as $W_{\mathcal{C}}(x, z) = \sum_{i=0}^{n} W_{i,n-i} z^i x^{n-i}$ where $W_{i,n-i}$ represents the number of codewords in $\mathcal{C}$ whose Hamming weight is i. The following result follows from Theorem 7.

Corollary 8. *Let $m+1$ be a prime integer. Let $\mathcal{C}$ be a single-mineral code created according to Construction B where the group-code partition is used and the $(m+1)$-ary constituent code $\mathcal{C}_1$ is a non-binary Hamming code of length n. Then $|\mathcal{C}| \leq \frac{2^{mn}}{mn+1} + \frac{mn 2^{(m(n-1))/(m+1)}}{mn+1}$.*

Proof: For the non-binary Hamming code $\mathcal{C}_1$ of length n defined over $GF(m+1)$, we have that $W_{\mathcal{C}_1}(x, z) = \frac{1}{mn+1} \left((x + mz)^n + mn(x - z)^{(mn+1)/(m+1)} z^{(n-1)/(m+1)} \right)$ ([13], Chapter 4). Substituting $x = \frac{2^m + m}{m+1}$ and $z = \frac{2^m - 1}{m+1}$ then gives the maximum number of codewords in the code $\mathcal{C}$ according to Theorem 7. ■

In the following remark, recall Π_m refers to the set of permutations of the symbols $\{0, 1, \ldots, m\}$.

Remark 4. *For a prime p, a positive integer r, and the Abelian group $\mathcal{A} = GF(p)^r$, it was shown in [2], Theorem 14, that the length $p^r - 1$ code $\mathcal{C}_0^{\mathcal{A}}$ satisfies $|\mathcal{C}_0^{\mathcal{A}}| = \frac{2^{p^r-1}}{p^r} + \frac{(p^r-1)2^{p^{r-1}-1}}{p^r}$. Let $\boldsymbol{a} = (0, 1, \ldots, p-1) \in \Pi_{p-1}$ and suppose $\mathcal{C}_1$ is a perfect code of length $\frac{p^r-1}{p-1}$ over $GF(p)$ so that $\mathcal{C}(\boldsymbol{a}, \mathcal{C}_1)$ has length $p^r - 1$. Then from Corollary 8, $|\mathcal{C}(\boldsymbol{a}, \mathcal{C}_1)| = |\mathcal{C}_0^{\mathcal{A}}|$.*

As noted in the previous remark, if Construction B is used to create a single-mineral code and $\mathcal{C}_1$ is a perfect and linear non-binary code, then (for a fixed length) Construction B does not result in codes that are any larger than the group codes. In the next section, we consider using perfect and linear non-binary single-random-error-correcting codes with different coloring schemes to construct larger codes.

C. A new coloring scheme

In this section, we report on the results of using Construction B with a new map that was located using a computerized search. As before, we denote the color classes as A_0, A_1, $\ldots$, A_{k-1} for the k-coloring $\Phi_{t,m}$ on $\mathcal{G}_{t,m}$. By this setup, we assume

1) $\forall j \in \{0, \ldots, k-1\}$, $A_j \subseteq GF(2)^m$,
2) for any $i, j \in \{0, \ldots, k-1\}$ where $i \neq j$ $A_i \cap A_j = \emptyset$,
3) $|A_0| \geq |A_1| \geq \ldots \geq |A_{k-1}|$.

In this subsection, we make use of the following notation. Suppose a code $\mathcal{C}$ is a t-mineral-error-correcting code created according to Construction B given by

1) a set of p color classes $D = \{A_0, A_1, \ldots, A_{p-1}\}$ for a p-coloring on $\mathcal{G}_{t,m}$ where p is a prime,
2) the mapping $\Phi_{t,m}$ which maps vectors from $GF(2)^m$ into the symbols $\{0, 1, \ldots, p-1\}$,
3) $\mathcal{C}_t$ where $\mathcal{C}_t$ is a t-random-error-correcting code over $GF(p)$.

We denote the mineral code $\mathcal{C}$ as $\mathcal{C}(D, \Phi_{t,m}, \mathcal{C}_t)$. Under this setup, the map $\Phi_{t,m}$ always maps elements from the same color class to the same symbol.

In the following, we describe the color classes from a 7-coloring on $\mathcal{G}_{1,6}$ that was located with the aid of a

computer search. The vectors from $GF(2)^m$ are enumerated by their decimal representation. For example, the vector $\boldsymbol{x} = (x_1, x_2, x_3, x_4, x_5, x_6) = (1, 0, 1, 1, 0, 0)$ corresponds to the number 13 since $\sum_{i=1}^{6} 2^{i-1} x_i = 13$ in this representation. The color classes are the following:

1) *Color class* A_0*:* $\{0, 3, 12, 15, 21, 24, 36, 43, 49, 54, 61\}$
2) *Color class* A_1*:* $\{2, 5, 14, 27, 42, 48, 55, 60\}$
3) *Color class* A_2*:* $\{1, 6, 13, 18, 25, 30, 37, 40, 59\}$
4) *Color class* A_3*:* $\{4, 7, 9, 19, 31, 34, 46, 52, 57\}$
5) *Color class* A_4*:* $\{8, 11, 20, 23, 33, 38, 45, 50, 62\}$
6) *Color class* A_5*:* $\{10, 16, 22, 28, 35, 41, 47, 53, 58\}$
7) *Color class* A_6*:* $\{17, 26, 29, 32, 39, 44, 51, 56, 63\}$.

Notice that $|A_0| = 11, |A_1| = 8, |A_2| = 9, |A_3| = 9, |A_4| = 9, |A_5| = 9$, and $|A_6| = 9$. Recall that if the group-code partition was used then the sizes of the color classes are $10, 9, 9, 9, 9, 9, 9$ so that the size of the largest color class has increased by 1 given the new set of color classes.

Using a non-binary perfect code over $GF(7)$ of length 8 with the coloring scheme mentioned in this section, the resulting length-48 binary code has 16192 more codewords than a group code defined over $\mathbb{Z}_7 \times \mathbb{Z}_7$. Using a non-binary perfect code over $GF(7)$ of length 57 with the coloring scheme described in this section results in a binary code of length 342 with approximately $7.1401e34$ more codewords than a group code defined over $\mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_7$. The parity check matrices for the single-random-error-correcting codes of length 8 and of length 57 over $GF(7)$ were taken from [16].

VII. Conclusion and Future Work

In this work, new bounds and constructions were derived for grain-error-correcting codes where the lengths of the grains were at most two. We considered a new approach to constructing codes that correct grain-errors and using this approach, we improved upon the constructions in [10] and [15].

There are many directions for future work:

1) Development of new coloring schemes and codes to use with Construction B.
2) Constructions of codes that correct multiple non-overlapping grain-errors.
3) Constructions and bounds for codes capable of correcting grain-errors where the length of the grain is greater than two.
4) Constructions and bounds for codes that correct bursts of grain-errors.

The largest single-grain codes for $9 \leq n \leq 15$ listed in Table I were the result of using Construction B with non-linear codes over $GF(3)$. It seems promising that potentially larger single-grain codes may be possible using non-linear codes and coloring schemes in conjunction with Construction B for longer code lengths.

There is clearly a strong connection between codes capable of correcting bursts of unidirectional errors and codes correcting grain-errors (where the length of the grain is longer than two). Constructing grain codes that are larger than the unidirectional codes from [12] could be of future research interest.

Finally, we note that Construction B may be applicable to the construction of new asymmetric error-correcting codes for the Z-channel. In fact, when $\Phi_{t,m} = \Gamma$ and $\mathcal{C}_1$ (from Construction B) is a single random-error-correcting ternary code, Construction B is identical to the single asymmetric error-correcting code (from the ternary construction) described in [5]. Given new colorings (i.e., where $\Phi_{1,m} \neq \Gamma$) and new ternary codes for $\mathcal{C}_1$, it may be possible to construct new codes with large cardinalities for the Z-channel.

Acknowledgements

The authors would like to thank Artyom Sharov for his helpful discussions about code cardinalities. Research supported in part by SMART scholarship, ISEF Foundation, and NSF grants CCF-1029030 and CCF-1150212.

References

[1] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, 2004.
[2] S. D. Constantin and T. R. M. Rao, "On the theory of binary asymmetric error-correcting codes," *Information and Control*, vol. 40, pp. 20-36, 1979.
[3] D. Cullina, A. A. Kulkarni, and N. Kiyavash, "A coloring approach to constructing deletion correcting codes from constant weight subgraphs," *Proc. IEEE International Symposium on Information Theory*, pp. 513-517, Boston, MA, 2012.
[4] R. Gabrys, E. Yaakobi, and L. Dolecek, "Correcting Grain-Errors in Magnetic Media," *Proc. IEEE International Symposium on Information Theory*, pp. 689-693, Istanbul, Turkey, 2013.
[5] M. Grassl, P. Shor, G. Smith, J. Smolin, and B. Zeng, "New constructions of codes for asymmetric channels via concatenation," *Proc. IEEE International Symposium on Information Theory*, pp. 751-755, Boston, MA, 2012.
[6] J. I. Hall, *Notes on Coding Theory*, available at http://www.mth.msu.edu/∼jhall/classes/codenotes/coding-notes.html, 2013.
[7] A. R. Iyengar, P. H. Siegel, and J. K. Wolf, "Write channel model for bit- patterned media recording," *IEEE Transactions on Magnetics*, vol. 47, no. 1, pp. 35-45, 2011.
[8] N. Kashyap and G. Zemor, "Upper bounds on the size of grain-correcting codes," available at *http://arxiv.org/abs/1302.6154*, 2013.
[9] A. A. Kulkarni and N. Kiyavash, "Non-asymptotic upper bounds for deletion correcting codes," available at *http://arxiv.org/abs/1211.3128*, 2012.
[10] A. Mazumdar, A. Barg, and N. Kashyap, "Coding for high-density recording on a 1-d granular magnetic medium," *IEEE Transactions on Information Theory*, vol. 57, no. 11, pp. 7403-7417, 2011.
[11] R. J. McEliece and E. R. Rodemich, "The Constantin-Rao construction for binary asymmetric error-correcting codes," *The Deep Space Network*, pp. 124-129, ID 19790016933, 1979.
[12] S. Park and B. Bose, "Burst asymmetric/unidirectional error correcting/detecting codes," *20th International Symposium on Fault-Tolerant Computing*, pp. 273-280, Newcastle Upon Tyne, UK, 1990.
[13] R. Roth, *Introduction to Coding Theory*, Cambridge University Press, 2006.
[14] J. J. Rotman, *An Introduction to the Theory of Groups*, Springer, 1994.
[15] A. Sharov and R. M. Roth, "Bounds and constructions for granular media coding," *Proc. IEEE International Symposium on Information Theory*, pp. 2343-2347, St. Petersburg, Russia, 2011.

[16] University of Sydney, *Magma Computational Algebra System, http://magma.maths.usyd.edu.au/magma/*, 2011.
[17] D. B. West, *Introduction to Graph Theory*, Prentice Hall Upper Saddle River, 2001, vol. 2.
[18] R. I. White, R. M. H. New and R. F. W. Pease, "Patterned media: viable route to 50Gb/in2 and up for magnetic recording," *IEEE Trans. Magnetics*, vol. 33, no. 1, pt. 2, pp. 990-995, Jan. 1997.
[19] R. Wood, M. Williams, A. Kavcic, and J. Miles, "The feasibility of magnetic recording at 10 terabits per square inch on conventional media," *IEEE Transactions on Magnetics*, vol. 45, no. 2, pp. 917-923, 2009.

APPENDIX A
PROOFS OF CLAIMS AND LEMMAS FROM SECTION III

A. Details for $M(n,2)$

For the bound on $M(n,2)$ stated in Lemma 6, the following two claims were used.

Claim 4. *For $n \geq 2$,*

$$\sum_{k=2}^{n} \frac{1}{k+1} \binom{n}{k} = \frac{1}{n+1}(2^{n+1} - 2 - \frac{3n}{2} - \frac{n^2}{2}).$$

Proof: This identity follows from the following derivations:

$$\sum_{k=2}^{n} \frac{1}{k+1} \binom{n}{k} = \sum_{k=0}^{n} \frac{1}{k+1} \binom{n}{k} - 1 - n/2$$
$$= \sum_{k=0}^{n} \frac{1}{n+1} \binom{n+1}{k+1} - 1 - n/2 = \frac{2^{n+1}-1}{n+1} - 1 - n/2$$
$$= \frac{1}{n+1}(2^{n+1} - 2 - \frac{3n}{2} - \frac{n^2}{2}).$$

■

Claim 5. *For $n \geq 14$,*

$$\sum_{k=1}^{n} \frac{1}{k} \binom{n}{k} \leq \frac{2^{n+1}}{n-1-\frac{2}{n-5}}.$$

Proof: This claim is proved by induction. We first verify that this claim holds for $n = 14$. The left hand side is equal 2562.01, while the right hand side is equal 2564.45, and so this inequality holds for $n = 14$.

Assume that this inequality holds for some $n \geq 14$ and we will prove it holds for $n+1$ as well. That is, we will show that $\sum_{k=1}^{n+1} \frac{1}{k} \binom{n+1}{k} \leq \frac{2^{n+2}}{n-\frac{2}{n-4}}$. Note that

$$\sum_{k=1}^{n+1} \frac{1}{k} \binom{n+1}{k} = \sum_{k=1}^{n+1} \frac{1}{k} \left(\binom{n}{k} + \binom{n}{k-1} \right)$$
$$= \sum_{k=1}^{n} \frac{1}{k} \binom{n}{k} + \sum_{k=1}^{n+1} \frac{1}{k} \binom{n}{k-1} = \sum_{k=1}^{n} \frac{1}{k} \binom{n}{k} + \sum_{k=1}^{n+1} \frac{1}{n+1} \binom{n+1}{k}$$
$$= \sum_{k=1}^{n} \frac{1}{k} \binom{n}{k} + \frac{2^{n+1}-1}{n+1}.$$

Now, according to the induction assumption we get that

$$\sum_{k=1}^{n+1} \frac{1}{k} \binom{n+1}{k} = \sum_{k=1}^{n} \frac{1}{k} \binom{n}{k} + \frac{2^{n+1}-1}{n+1}$$
$$\leq \frac{2^{n+1}}{n-1-\frac{2}{n-5}} + \frac{2^{n+1}}{n+1} = 2^{n+2} \cdot \frac{n - \frac{1}{n-5}}{(n-1-\frac{2}{n-5})(n+1)}.$$

Next, we note that for $n \geq 14$, $\frac{n-\frac{1}{n-5}}{(n-1-\frac{2}{n-5})(n+1)} \leq \frac{1}{n-\frac{2}{n-4}}$, and therefore we conclude that

$$\sum_{k=1}^{n+1} \frac{1}{k} \binom{n+1}{k} \leq \frac{2^{n+2}}{n-\frac{2}{n-4}}.$$

■

B. Details for $M(n,3)$

Our next step is to derive similar results for $M(n,3)$. We apply a slightly different approach in our calculation this time. First, we note to the following identity

Claim 12. *For $n \geq 1$, $\sum_{k=1}^{n} \frac{1}{k}\binom{n}{k} = \sum_{k=1}^{n} \frac{2^k-1}{k}$.*

Proof: We will prove this claim by induction as well. For $n = 1$ both terms are equal to 1 and thus the equality holds. Let us assume that the equation holds for some $n \geq 1$ and we will prove it holds for $n+1$, that is, we will show that $\sum_{k=1}^{n+1} \frac{1}{k}\binom{n+1}{k} = \sum_{k=1}^{n+1} \frac{2^k-1}{k}$. Similarly to the proof of Claim 5, we have that

$$\sum_{k=1}^{n+1} \frac{1}{k} \binom{n+1}{k} = \sum_{k=1}^{n} \frac{1}{k} \binom{n}{k} + \frac{2^{n+1}-1}{n+1},$$

and according to the induction assumption we get

$$\sum_{k=1}^{n+1} \frac{1}{k} \binom{n+1}{k} = \sum_{k=1}^{n} \frac{2^k-1}{k} + \frac{2^{n+1}-1}{n+1} = \sum_{k=1}^{n+1} \frac{2^k-1}{k}.$$

■

Note that according to Claim 5 and Claim 12 we can deduce that $\sum_{k=1}^{n} \frac{2^k-1}{k} \leq \frac{2^{n+1}}{n-1-\frac{2}{n-5}}$. However, we will have to use a slightly better upper bound here, which is proved next.

Lemma 13. *For $n \geq 17$,*

$$\sum_{k=1}^{n} \frac{2^k-1}{k} \leq \frac{2^{n+1}}{n-1-\frac{2}{n-5}+\frac{1}{n^2}}.$$

Proof: For $n = 17$, the value on the left hand side is equal 16552.47, while the value of the right hand side is equal 16552.85. Now, assume the inequality holds for some $n \geq 17$, and we will show its validity for $n+1$. Hence, we need to show that

$$\sum_{k=1}^{n+1} \frac{2^k-1}{k} \leq \frac{2^{n+2}}{n-\frac{2}{n-4}+\frac{1}{(n+1)^2}}.$$

According to the induction assumption, it is enough to show that

$$\frac{2^{n+1}}{n-1-\frac{2}{n-5}+\frac{1}{n^2}} + \frac{2^{n+1}-1}{n+1} \leq \frac{2^{n+2}}{n-\frac{2}{n-4}+\frac{1}{(n+1)^2}},$$

or

$$\frac{1}{n-1-\frac{2}{n-5}+\frac{1}{n^2}}+\frac{1}{n+1}\leq\frac{2}{n-\frac{2}{n-4}+\frac{1}{(n+1)^2}},$$

which holds for $n\geq 17$. ■

The next claim will be useful in the derivation of the bound on $M(n,3)$.

Lemma 14. *For* $n\geq 2$,

$$\sum_{k=2}^{n}\frac{1}{k-1}\binom{n}{k}=n\sum_{k=1}^{n-1}\frac{2^k-1}{k}-2^n+n+1.$$

Proof: For $n\geq 1$, we denote $A(n)=\sum_{k=2}^{n}\frac{1}{k-1}\binom{n}{k}$, where $A(1)=0$, and $B(n)=\sum_{k=1}^{n}\frac{1}{k}\binom{n}{k}$. We note that

$$A(n)=\sum_{k=2}^{n}\frac{1}{k-1}\binom{n}{k}=\sum_{k=2}^{n}\frac{1}{k-1}\left(\binom{n-1}{k}+\binom{n-1}{k-1}\right)$$
$$=\sum_{k=2}^{n-1}\frac{1}{k-1}\binom{n-1}{k}+\sum_{k=1}^{n-1}\frac{1}{k}\binom{n-1}{k}=A(n-1)+B(n-1).$$

Therefore, according to Claim 12 we get

$$A(n)=\sum_{i=1}^{n-1}B(i)=\sum_{i=1}^{n-1}\sum_{k=1}^{i}\frac{1}{k}\binom{i}{k}=\sum_{i=1}^{n-1}\sum_{k=1}^{i}\frac{2^k-1}{k}$$
$$=\sum_{k=1}^{n-1}\frac{2^k-1}{k}(n-k)=n\sum_{k=1}^{n-1}\frac{2^k-1}{k}-\sum_{k=1}^{n-1}(2^k-1)$$
$$=n\sum_{k=1}^{n-1}\frac{2^k-1}{k}-\left(2^n-n-1\right).$$

■

Lemma 15. *For* $n\geq 24$,

$$M(n,3)\leq 2\left\lfloor 3\cdot 2^n\left(\frac{8+\frac{44}{n-7}+\frac{1}{n}-\frac{2}{(n-2)^2}}{n(n-1)(n-3-\frac{2}{n-7}+\frac{2}{(n-2)^2})}\right)\right\rfloor.$$

Proof: From Theorem 1 we have

$$M(n,3)=2\sum_{k=0}^{n-1}\binom{n-1}{k}\frac{1}{\sum_{j=0}^{\min\{3,k\}}\binom{k}{j}}$$
$$=2+n-1+\frac{1}{2}\cdot\binom{n-1}{2}+2\sum_{k=3}^{n-1}\binom{n-1}{k}\frac{1}{1+k+\binom{k}{2}+\binom{k}{3}}$$
$$\leq\frac{n^2+n+6}{4}+2\sum_{k=3}^{n-1}\binom{n-1}{k}\frac{1}{\binom{k}{2}+\binom{k}{3}}$$
$$=\frac{n^2+n+6}{4}+12\sum_{k=3}^{n-1}\binom{n-1}{k}\left(\frac{1/2}{k-1}-\frac{1}{k}+\frac{1/2}{k+1}\right)$$
$$=\frac{n^2+n+6}{4}+6\sum_{k=3}^{n-1}\binom{n-1}{k}\frac{1}{k-1}$$
$$-12\sum_{k=3}^{n-1}\binom{n-1}{k}\frac{1}{k}+6\sum_{k=3}^{n-1}\binom{n-1}{k}\frac{1}{k+1}.$$

According to Lemma 14,

$$\sum_{k=3}^{n-1}\binom{n-1}{k}\frac{1}{k-1}=(n-1)\sum_{k=1}^{n-2}\frac{2^k-1}{k}-2^{n-1}-\frac{n^2-5n+2}{2}.$$

By Claim 12,

$$\sum_{k=3}^{n-1}\binom{n-1}{k}\frac{1}{k}=\sum_{k=1}^{n-1}\frac{2^k-1}{k}-\frac{n^2+n-2}{4},$$

and by Claim 4,

$$\sum_{k=3}^{n-1}\binom{n-1}{k}\frac{1}{k+1}=\frac{1}{n}\left(2^n-2-\frac{3(n-1)}{2}-\frac{(n-1)^2}{2}\right)$$
$$-\frac{n^2-3n+2}{6}.$$

All together we get that

$$M(n,3)\leq\frac{n^2+n+6}{4}$$
$$+6\left((n-1)\sum_{k=1}^{n-2}\frac{2^k-1}{k}-2^{n-1}-\frac{n^2-5n+2}{2}\right)$$
$$-12\left(\sum_{k=1}^{n-1}\frac{2^k-1}{k}-\frac{n^2+n-2}{4}\right)$$
$$+6\left(\frac{1}{n}\left(2^n-2-\frac{3(n-1)}{2}-\frac{(n-1)^2}{2}\right)-\frac{n^2-3n+2}{6}\right)$$
$$=-\frac{3n^2}{4}+\frac{73n}{4}-\frac{31}{2}-\frac{6}{n}+6(n-1)\sum_{k=1}^{n-2}\frac{2^k-1}{k}-3\cdot 2^n$$
$$-12\sum_{k=1}^{n-1}\frac{2^k-1}{k}+\frac{6\cdot 2^n}{n}$$
$$=-\frac{3n^2}{4}+\frac{73n}{4}-\frac{31}{2}-\frac{6}{n}+6(n-3)\sum_{k=1}^{n-2}\frac{2^k-1}{k}-3\cdot 2^n$$
$$-12\cdot\frac{2^{n-1}-1}{n-1}+\frac{6\cdot 2^n}{n}$$
$$\leq 6(n-3)\sum_{k=1}^{n-2}\frac{2^k-1}{k}-3\cdot 2^n-\frac{6\cdot 2^n}{n-1}+\frac{6\cdot 2^n}{n}$$
$$=6(n-3)\sum_{k=1}^{n-2}\frac{2^k-1}{k}-3\cdot 2^n-\frac{6\cdot 2^n}{n(n-1)}$$

where the inequality holds for $n\geq 24$. Finally, according to Lemma 13 we finally get

$$M(n,3)\leq 6(n-3)\frac{2^{n-1}}{n-3-\frac{2}{n-7}+\frac{2}{(n-2)^2}}-3\cdot 2^n-\frac{6\cdot 2^n}{n(n-1)}$$
$$=2^n\left(\frac{3n-9}{n-3-\frac{2}{n-7}+\frac{2}{(n-2)^2}}-3-\frac{6}{n(n-1)}\right)$$
$$=2^n\left(\frac{\frac{6}{n-7}-\frac{6}{(n-2)^2}}{n-3-\frac{2}{n-7}+\frac{2}{(n-2)^2}}-\frac{6}{n(n-1)}\right)$$
$$=6\cdot 2^n\left(\frac{8+\frac{44}{n-7}+\frac{1}{n}-\frac{2}{(n-2)^2}}{n(n-1)(n-3-\frac{2}{n-7}+\frac{2}{(n-2)^2})}\right).$$

From Lemma 4, $M(n,2)$ must be an even integer and so $M(n,3)\leq 2\left\lfloor 3\cdot 2^n\left(\frac{8+\frac{44}{n-7}+\frac{1}{n}-\frac{2}{(n-2)^2}}{n(n-1)(n-3-\frac{2}{n-7}+\frac{2}{(n-2)^2})}\right)\right\rfloor$.

■

Appendix B
Proof of Claim 9

In this section, prove the correctness of Claim 9. The approach used will be the same as that in ([6], Chapter 9) and ([13], Chapter 4), and the material is included here for completeness.

Recall from Section VI-B, we write the complete weight enumerator of a code $\mathcal{C}$ as $W_{\mathcal{C}}(z_0, \ldots, z_{p-1}) = \sum_{i_0, i_1, \ldots, i_{p-1}} W_{i_0, \ldots, i_{p-1}} z_0^{i_0} \cdots z_{p-1}^{i_{p-1}}$ where $W_{i_0, \ldots, i_{p-1}}$ denotes the number of codewords in a code $\mathcal{C}$ that have exactly i_0 symbols of value 0, i_1 symbols of value 1, and so on.

Suppose ζ_p is a p-th root of unity. Then the complete weight enumerator of a code $\mathcal{C}$ of length n defined over $GF(p)$ can be expressed in terms of the codewords in the dual code $\mathcal{C}^{\perp}$ as follows. For shorthand, let $W_{\mathcal{C}}(z_0, \ldots z_{p-1}) = W_{\mathcal{C}}(\boldsymbol{z})$. First, note that for $\boldsymbol{v} \in GF(p)^n$,

$$\sum_{\boldsymbol{x} \in \mathcal{C}^{\perp}} \zeta_p^{\boldsymbol{v}^T \cdot \boldsymbol{x}} = \begin{cases} |\mathcal{C}^{\perp}| & \text{if } \boldsymbol{v} \in \mathcal{C}, \\ 0 & \text{otherwise.} \end{cases} \tag{17}$$

Let $I_{\mathcal{C}} : GF(p)^n \to \{0, 1\}$ denote the indicator function where for $\boldsymbol{x} \in GF(p)^n$

$$I_{\mathcal{C}}(\boldsymbol{x}) = \begin{cases} 1 & \text{if } \boldsymbol{x} \in \mathcal{C}, \\ 0 & \text{otherwise.} \end{cases} \tag{18}$$

Then,

$$\begin{aligned}
W_{\mathcal{C}}(\boldsymbol{z}) &= \sum_{\boldsymbol{v} \in GF(p)^n} I_{\mathcal{C}}(\boldsymbol{v}) W_{\{\boldsymbol{v}\}}(\boldsymbol{z}) \\
&= \sum_{\boldsymbol{v} \in GF(p)^n} \frac{1}{|\mathcal{C}^{\perp}|} \left(\sum_{\boldsymbol{x} \in \mathcal{C}^{\perp}} \zeta_p^{\boldsymbol{v}^T \cdot \boldsymbol{x}} \right) W_{\{\boldsymbol{v}\}}(\boldsymbol{z}) \\
&= \frac{1}{|\mathcal{C}^{\perp}|} \sum_{\boldsymbol{x} \in \mathcal{C}^{\perp}} \sum_{\boldsymbol{v} \in GF(p)^n} \zeta_p^{\boldsymbol{v}^T \cdot \boldsymbol{x}} W_{\{\boldsymbol{v}\}}(\boldsymbol{z}) \\
&= \frac{1}{|\mathcal{C}^{\perp}|} \sum_{\boldsymbol{x} \in \mathcal{C}^{\perp}} \sum_{\boldsymbol{v} \in GF(p)^n} \prod_{i=1}^{n} \zeta_p^{v_i x_i} W_{\{v_i\}}(\boldsymbol{z}) \\
&= \frac{1}{|\mathcal{C}^{\perp}|} \sum_{\boldsymbol{x} \in \mathcal{C}^{\perp}} \prod_{i=1}^{n} \sum_{v_i \in GF(p)} \zeta_p^{v_i x_i} W_{\{v_i\}}(\boldsymbol{z}) \\
&= \frac{1}{|\mathcal{C}^{\perp}|} \sum_{\boldsymbol{x} \in \mathcal{C}^{\perp}} \prod_{i=1}^{n} \left(z_0 + \zeta_p^{1 \cdot x_i} z_1 + \ldots + \zeta_p^{(p-1) \cdot x_i} z_{p-1} \right).
\end{aligned}$$