Near MDS poset codes and distributions

Alexander Barg*
Dept. of ECE and Institute for Systems Research
University of Maryland, College Park, MD 20742
abarg@umd.edu

Punarbasu Purkayastha*
Dept. of ECE
University of Maryland, College Park, MD 20742
ppurka@umd.edu

***Abstract*—We study q-ary codes with distance defined by a partial order of the coordinates of the codewords. Maximum Distance Separable (MDS) codes in the poset metric have been studied in a number of earlier works. We consider codes that are close to MDS codes by the value of their minimum distance. For such codes, we determine their weight distribution, and in the particular case of the "ordered metric" characterize distributions of points in the unit cube defined by the codes. We also give some constructions of codes in the ordered Hamming space.**

I. Introduction

A set of points $C = \{c_1, \dots, c_M\}$ in the q-ary n-dimensional Hamming space $\mathbb{F}_q^n$ is called a Maximum Distance Separable (MDS) code if the Hamming distance between any two distinct points of C satisfies $d(c_i, c_j) \geq d$ and the number of points is $M = q^{n-d+1}$. By the well-known Singleton bound of coding theory, this is the maximum possible number of points with the given separation. If C is an MDS code that forms an $\mathbb{F}_q$-linear space, then its dimension k, distance d and length n satisfy the relation $d = n-k+1$. MDS codes are known to be linked to classical old problems in finite geometry and to a number of other combinatorial questions related to the Hamming space [13]. At the same time, the length of MDS codes cannot be very large; in particular, in all the known cases, $n \leq q + 2$. This restriction has led to the study of classes of codes with distance properties close to MDS codes, such as t-th rank MDS codes [16], near MDS codes [4] and almost MDS codes [3]. The distance of these codes is only slightly less than $n - k + 1$, and at the same time they still have many of the structural properties associated with MDS codes.

In this paper we extend the study of near MDS (NMDS) codes to the case of the ordered Hamming space and more generally, to poset metrics. The ordered Hamming space was introduced independently by Niederreiter [11] for the purpose of studying uniform distributions of points in the unit cube, and by Rosenbloom and Tsfasman [12] for a study of one generalization of Reed-Solomon codes (the ordered distance is therefore sometimes called the NRT distance). A particular class of distributions in $U^n = [0, 1)^n$, called (t, m, n)-nets, defined by Niederreiter in the course of his studies, presently forms the subject of a large body of literature. MDS codes in the ordered Hamming space and their relations to distributions and (t, m, n)-nets have been extensively studied [12], [14], [5], [7]. The ordered Hamming space was further generalized by Brualdi et al. in [2] which introduced metrics on strings defined by arbitrary partially ordered sets, calling them poset metrics.

* Supported in part by NSF grants DMS0807411, CCF0916919, CCF0830699, and CCF0635271.

The relation between MDS and NMDS codes in the ordered metric and distributions is the main motivation of the present study. As was observed by Skriganov [14], MDS codes correspond to optimal uniform distributions of points in the unit cube. The notion of uniformity is rather intuitive: an allocation of M points forms a uniform distribution if every measurable subset $A \subset U^n$ contains a $\mathrm{vol}(A)$ proportion of the M points (in distributions that arise from codes, this property is approximated by requiring that it hold only for some fixed collection of subsets). Skriganov [14] observes that distributions that arise from MDS codes are optimal in some well-defined sense. In the same way, NMDS codes correspond to distributions that are not far from optimal (they are characterized exactly below).

The rest of the article is organized as follows. In the next section we provide basic definitions and some properties of near-MDS codes. We will also have a chance to discuss generalized Hamming weights of Wei [16] in the poset metric case. In Section III we show a relationship between distribution of points in the unit cube and NMDS codes. In Section IV we determine the weight distribution of NMDS codes, and finally in Section V, we provide some constructions of NMDS codes in the ordered Hamming space.

II. Definitions and basic properties

A. Poset metrics

We begin with defining poset metrics on q-ary strings of a fixed length and introduce the ordered Hamming metric as a special case of the general definition. Entries of a string $x = (x_1, x_2, \dots)$ are indexed by a finite set N which we call the set of coordinates. Let $\overrightarrow{\mathcal{P}}$ be an arbitrary partial order ($\leq$) on N. Together N and $\overrightarrow{\mathcal{P}}$ form a *poset*. An *ideal* of the poset is a subset $I \subset N$ that is "downward closed" under the $\leq$ relation, which means that the conditions $i, j \in N$, $j \in I$ and $i \leq j$ imply that $i \in I$. For the reasons that will become clear below, such ideals will be called *left-adjusted* (l.a.).

A chain is a linearly ordered subset of the poset. The *dual poset* $\overleftarrow{\mathcal{P}}$ is the set N with the same set of chains as $\overrightarrow{\mathcal{P}}$, but the order within each of them reversed. In other words $j \leq i$ in $\overleftarrow{\mathcal{P}}$ if and only if $i \leq j$ in $\overrightarrow{\mathcal{P}}$. An ideal in the dual poset will

be termed *right-adjusted* (r.a.). For a subset $S \subseteq \overrightarrow{\mathcal{P}}$ we denote by $\langle S\rangle = \langle S\rangle_{\overrightarrow{\mathcal{P}}}$ the smallest $\overrightarrow{\mathcal{P}}$-ideal containing the set S (we write $S \subseteq \overrightarrow{\mathcal{P}}$ to refer to a subset $S \subseteq N$ whose elements are ordered according to $\overrightarrow{\mathcal{P}}$). The support of a sequence x is the subset $\operatorname{supp} x \subseteq N$ formed by the indices of all the nonzero entries of x. The set $\langle \operatorname{supp} x\rangle \subseteq \overrightarrow{\mathcal{P}}$ will be called the l.a. support of x. The r.a. support is defined analogously.

Definition 2.1: (Brualdi et al. [2]) Let $\overrightarrow{\mathcal{P}}$ be a poset defined on N and let $x, y \in \mathbb{F}_q^{|N|}$ be two strings. Define the weight of x with respect to $\overrightarrow{\mathcal{P}}$ as $\mathrm{w}(x) = \langle \operatorname{supp} x\rangle$, i.e., the size of the smallest $\overrightarrow{\mathcal{P}}$-ideal that contains the support of x. The distance between x and y is defined as $d_{\overrightarrow{\mathcal{P}}}(x, y) = \mathrm{w}(x-y) = |\langle \operatorname{supp}(x-y)\rangle|$.

A code $\mathcal{C}$ of minimum distance d is a subset of $\mathbb{F}_q^{|N|}$ such that any two distinct vectors x and y of $\mathcal{C}$ satisfy $d_{\overrightarrow{\mathcal{P}}}(x, y) \geq d$. It is similarly possible to consider codes whose distance is measured relative to $\overleftarrow{\mathcal{P}}$. Given a linear code $\mathcal{C} \subset \mathbb{F}_q^{|N|}$ its *dual code* $\mathcal{C}^\perp$ is the set of vectors $\{y \in \mathbb{F}_q^{|N|} : \forall_{x\in\mathcal{C}} \ \sum_i x_i y_i = 0\}$. The weights in the dual code $\mathcal{C}^\perp$ are considered with respect to the dual poset $\overleftarrow{\mathcal{P}}$.

A subset of $\mathbb{F}_q^{|N|}$ is called an *orthogonal array* of strength t and index θ with respect to $\overrightarrow{\mathcal{P}}$ if any t l.a. columns contain any vector $z \in \mathbb{F}^t$ exactly θ times. In particular, the dual of a *linear* poset code is also a *linear* orthogonal array.

For instance, the Hamming metric is defined by the partial order $\overrightarrow{\mathcal{P}}$ which is a single antichain of length $n = |N|$ (no two elements are comparable). Accordingly, the distance between two sequences is given by the number of coordinates in which they differ. In this case, $\overrightarrow{\mathcal{P}} = \overleftarrow{\mathcal{P}}$.

B. Ordered Hamming metric

The *ordered Hamming metric* is defined by a poset $\overrightarrow{\mathcal{P}}$ which is a disjoint union of n chains of equal length r. Since we work with this metric in later sections of the paper, let us discuss it in more detail. In this case N is a union of n blocks of length r, and it is convenient to write a vector (sequence) as $x = (x_{11}, \ldots, x_{1r}, \ldots, x_{n1}, \ldots, x_{nr}) \in \mathbb{F}_q^{r,n}$. According to Definition 2.1, the weight of x is given by

$$\mathrm{w}(x) = \sum_{i=1}^{n} \max(j : x_{ij} \neq 0).$$

For a given vector x let $e_i, i = 1, \ldots, r$ be the number of r-blocks of x whose rightmost nonzero entry is in the ith position counting from the beginning of the block. The r-vector $e = (e_1, \ldots, e_r)$ will be called the *shape* of x. For brevity we will write

$$|e| = \sum_i e_i, \quad |e|' = \sum_i i e_i, \quad e_0 = n - |e|.$$

For $I = \langle \operatorname{supp} x\rangle$ we will denote the shape of the ideal I as shape(I)$= e$. By analogy with the properties of ideals in the ordered Hamming space, we use the term "left adjusted" for ideals in general posets $\overrightarrow{\mathcal{P}}$.

An (nr, M, d) *ordered code* $\mathcal{C} \subset \mathbb{F}_q^{r,n}$ is an arbitrary subset of M vectors in $\mathbb{F}_q^{r,n}$ such that the ordered distance between any two distinct vectors in $\mathcal{C}$ is at least d. If $\mathcal{C}$ is a linear code of dimension k over $\mathbb{F}_q$ and minimum ordered distance d, we will denote it as an $[nr, k, d]$ code. The dual of $\mathcal{C}$, denoted as $\mathcal{C}^\perp$, is defined as $\mathcal{C}^\perp = \{x \in \mathbb{F}_q^{r,n} : \forall_{c\in\mathcal{C}} \ \sum_{i,j} x_{ij} c_{ij} = 0\}$. The distance in $\mathcal{C}^\perp$ is derived from the dual order $\overleftarrow{\mathcal{P}}$, i.e., from the r.a. ideals.

The notion of orthogonal arrays in the ordered Hamming space is derived from the general definition. They will be called *ordered orthogonal arrays* (OOAs) below. We write (t, n, r, q) OOA for an orthogonal array of strength t in $\mathbb{F}_q^{r,n}$. Combinatorics of the ordered Hamming space and the duality between codes and OOAs was studied in detail by Martin and Stinson [9], Skriganov [14], and the present authors [1].

C. NMDS poset codes

We begin our study of NMDS codes in the poset space with several definitions that are generalized directly from the corresponding definitions in the Hamming space [16], [4]. The t-th *generalized poset weight* of a linear $[n, k]$ code $\mathcal{C}$ is defined as

$$d_t(\mathcal{C}) \triangleq \min\{|\langle \operatorname{supp} \mathcal{D}\rangle| : \mathcal{D} \text{ is an } [n, t] \text{ subcode of } \mathcal{C}\},$$

where $\operatorname{supp} \mathcal{D}$ is the union of the supports of all the vectors in $\mathcal{D}$. Note that $d_1(\mathcal{C}) = d$, the minimum distance of the code $\mathcal{C}$. Generalized poset weights have properties analogous to the well-known set of properties of generalized Hamming weights.

Lemma 2.2: Let $\mathcal{C}$ be a linear $[n, k]$ poset code in $\mathbb{F}_q^n$. Then

1) $0 < d_1(\mathcal{C}) < d_2(\mathcal{C}) < \cdots < d_k(\mathcal{C}) \leq n$.
2) Generalized Singleton bound: $d_t(\mathcal{C}) \leq n-k+t, \ \forall t \geq 1$.
3) If $\mathcal{C}^\perp$ is the dual code of $\mathcal{C}$ then

$$(n + 1 - \{d_1(\mathcal{C}^\perp), d_2(\mathcal{C}^\perp), \ldots, d_{n-k}(\mathcal{C}^\perp)\}) \cup \{d_1(\mathcal{C}), d_2(\mathcal{C}), \ldots, d_k(\mathcal{C})\} = \{1, \ldots, n\}. \quad (1)$$

4) Let H be the parity check matrix of $\mathcal{C}$. Then $d_t(\mathcal{C}) = \delta$ if and only if

a) Every $\delta - 1$ l.a. columns of H have rank at least $\delta - t$.
b) There exist δ l.a. columns of H with rank exactly $\delta - t$.

Definition 2.3: A linear code $\mathcal{C}[n, k, d]$ is called NMDS if $d(\mathcal{C}) = n - k$ and $d_2(\mathcal{C}) = n - k + 2$.

The next set of properties of NMDS codes can be readily obtained as generalizations of the corresponding properties of NMDS codes in the Hamming space [4].

Lemma 2.4: Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a linear $[n, k, d]$ code in the poset $\overrightarrow{\mathcal{P}}$.

1) $\mathcal{C}$ is NMDS if and only if
   a) Any $n - k - 1$ l.a. columns of the parity check matrix H are linearly independent.
   b) There exist $n - k$ l.a. linearly dependent columns of H.
   c) Any l.a. $n - k + 1$ columns of H are full ranked.
2) If $\mathcal{C}$ is NMDS, so is its dual $\mathcal{C}^\perp$.
3) $\mathcal{C}$ is NMDS if and only if $d(\mathcal{C}) + d(\mathcal{C}^\perp) = n$.
4) If $\mathcal{C}$ is NMDS then there exists an NMDS code with parameters $[n - 1, k - 1, d]$ and an NMDS code with parameters $[n - 1, k, d]$.

Lemma 2.5: Let $\mathcal{C}$ be a linear poset code in $\overrightarrow{\mathcal{P}}$ with distance d and let $\mathcal{C}^{\perp}$ be its dual code. Then the matrix M whose rows are the codewords of $\mathcal{C}^{\perp}$ forms an orthogonal array of strength $d-1$ with respect to $\overrightarrow{\mathcal{P}}$.

Proof: Follows because (1), $\mathcal{C}^{\perp}$ is the linear span of the parity-check matrix H of $\mathcal{C}$; and (2), any $d-1$ l.a. columns of H are linearly independent. ∎

III. NMDS CODES AND DISTRIBUTIONS

In this section we prove a characterization of NMDS poset codes and then use this result to establish a relationship between NMDS codes in the ordered Hamming space $\mathbb{F}_q^{r,n}$ and uniform distributions of points in the unit cube U^n. In our study of NMDS codes in the following sections, we analyze the properties of the code simultaneously as a linear code and as a linear orthogonal array.

Define the I-neighborhood of a poset code $\mathcal{C}$ with respect to an ideal I as

$$B_I(\mathcal{C}) = \bigcup_{c\in\mathcal{C}} B_I(c),$$

where $B_I(x) = \{v \in \mathbb{F}_q^n : \mathrm{supp}(v-x) \subseteq I\}$. We will say that a linear k-dimensional code $\mathcal{C}$ forms an *I-tiling* if there exists a partition $\mathcal{C} = \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_{q^{k-1}}$ into equal parts such that the I-neighborhoods of its parts are disjoint. If in addition the I-neighborhoods form a partition of $\mathbb{F}_q^n$, we say $\mathcal{C}$ forms a *perfect I-tiling*.

Theorem 3.1: Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be an $[n,k,d]$ linear code in the poset $\overrightarrow{\mathcal{P}}$. $\mathcal{C}$ is NMDS if and only if

1) For any $I \subset \overrightarrow{\mathcal{P}}, |I| = n-k+1$, the code $\mathcal{C}$ forms a perfect I-tiling.
2) There exists an ideal $I \subset \overrightarrow{\mathcal{P}}, |I| = n-k$ with respect to which $\mathcal{C}$ forms an I-tiling. No smaller-sized ideals with this property exist.

Proof: Let $\mathcal{C}$ be NMDS and let I be an ideal of size $n-k+1$. Let $H[I]$ be the submatrix of the parity-check matrix H of $\mathcal{C}$ obtained from H by deleting all the columns not in I. Since $\mathrm{rk}(H[I]) = n-k$, the space $\ker(H[I])$ is one-dimensional. Let $\mathcal{C}_1 = \ker(H(I))$ and let $\mathcal{C}_j$ be the jth coset of $\mathcal{C}_1$ in $\mathcal{C}$, $j = 2,\ldots,q^{k-1}$. The code $\mathcal{C}$ forms an orthogonal array of strength $k-1$ and index q in $\overleftarrow{\mathcal{P}}$. Therefore, every vector $z \in \mathbb{F}_q^{k-1}$ appears exactly q times in the restrictions of the codevectors $c \in \mathcal{C}$ to the coordinates of $J = I^c$. Thus, $c'[J] = c''[J]$ for any two vectors $c', c'' \in \mathcal{C}_i, i = 1,\ldots,q^{k-1}$ and $c'[J] \neq c''[J]$ $c' \in \mathcal{C}_i, c'' \in \mathcal{C}_j, 1 \le i < j \le q^{k-1}$. This implies that $\mathcal{C}$ forms a perfect I-tiling, which proves assumption 1 of the theorem. To prove assumption 2, repeat the above argument taking I to be the support of a minimum-weight codeword in $\mathcal{C}$.

To prove the converse, let $I \subseteq \overrightarrow{\mathcal{P}}$, $|I| = n-k+1$ be an ideal and let $\mathcal{C}_1,\ldots,\mathcal{C}_{q^{k-1}}$ be a partition of $\mathcal{C}$ with $|\mathcal{C}_i| = q$ for all i, that forms a perfect $I-$tiling. This implies that $c'[I^c] \neq c''[I^c]$, $c' \in \mathcal{C}_i, c'' \in \mathcal{C}_j, 1 \le i < j \le q^{k-1}$. In other words, $\mathcal{C}$ forms an orthogonal array with respect to $\overleftarrow{\mathcal{P}}$ of index q and strength $k-1$. We conclude that $d(\mathcal{C}^{\perp}) = k$ or $k+1$. If it is the latter, then $\mathcal{C}^{\perp}$ is MDS with respect to $\overleftarrow{\mathcal{P}}$ and so is $\mathcal{C}$ with respect to $\overrightarrow{\mathcal{P}}$, in violation of assumption 2. So $d(\mathcal{C}^{\perp}) = k$ and $d(\mathcal{C}) \le n-k$. If the inequality is strict, there exists an ideal I of size $< n-k$ that supports a one-dimensional subcode of $\mathcal{C}$. Then $\mathcal{C}$ forms an I-tiling which contradicts assumption 2.

It remains to prove that $d_2(\mathcal{C}) = n-k+2$. Assume the contrary, i.e., that there exists a 2-dimensional subcode $\mathcal{B} \subset \mathcal{C}$ whose l.a. support forms an ideal $I \subset \overrightarrow{\mathcal{P}}$ of size $n-k+1$. The q^2 vectors of $\mathcal{B}$ all have zeros in I^c which contradicts the fact that $\mathcal{C}$ forms an orthogonal array of index q. ∎

Next, we use this characterization to relate codes in the ordered Hamming space $\mathbb{F}_q^{r,n}$ to distributions. An idealized uniformly distributed point set $\mathcal{C}$ would satisfy the property that for any measurable subset $A \subset U^n$, $\frac{1}{|\mathcal{C}|}\sum_{x\in\mathcal{C}} 1(x \in A) = \mathrm{vol}(A)$. Distributions that we consider, and in particular (t,m,n)-nets, approximate this property by restricting the subsets A to be boxes with sides parallel to the coordinate axes.

Let $\mathcal{E} \triangleq \left\{ \prod_{i=1}^n \left[\frac{a_i}{q^{l_i}}, \frac{a_i+1}{q^{l_i}}\right) : 0 \le a_i < q^{l_i}, 0 \le l_i \le r, 1 \le i \le n \right\}$ be a collection of elementary intervals in the unit cube $U^n = [0,1)^n$. An arbitrary collection of q^k points in U^n is called an $[nr,k]$ *distribution* in the base q (with respect to $\mathcal{E}$). A distribution is called *optimal* if every elementary interval of volume q^{-k} contains exactly one point [14]. A related notion of (t,m,n) nets, introduced by Niederreiter [11], is obtained if we remove the upper bound on l_i (i.e., allow that $0 \le l_i < \infty$) and require that every elementary interval of volume q^{t-m} contain exactly q^t points.

An ordered code gives rise to a distribution of points in the unit cube via the following procedure. A codevector $(c_{11},\ldots,c_{1r},\ldots,c_{n1},\ldots,c_{nr}) \in \mathbb{F}_q^{r,n}$ is mapped to $x = (x_1,\ldots,x_n) \in U^n$ by letting

$$x_i = \sum_{j=1}^{r} c_{ij} q^{j-r-1}, 1 \le i \le n. \tag{2}$$

In particular, an $(m-t,n,r,q)$ OOA of index q^t and size q^m corresponds to a distribution in which every elementary interval of volume q^{t-m} contains exactly q^t points, and an $(m-t,n,m-t,q)$ OOA of index q^t and size q^m gives rise to a (t,m,n)-net [8], [10].

Proposition 3.2: (Skriganov [14]) An $[nr,k,d]$ MDS code in the ordered metric exists if and only if there exists an optimal $[nr,k]$ distribution.

Skriganov [15] also considers the concept of *nearly-MDS* codes whose distance asymptotically tends to the distance of MDS codes, and shows how these codes can give rise to distributions.

The next theorem whose proof is immediate from Theorem 3.1 relates ordered NMDS codes and distributions.

Theorem 3.3: Let $\mathcal{C}$ be a linear $[nr,k,d]$ code in $\mathbb{F}_q^{r,n}$ and let $P(\mathcal{C})$ be the corresponding set of points in U^n. Then $\mathcal{C}$ is NMDS if and only if

1) Any elementary interval of volume $q^{-(k-1)}$ has exactly q points of $P(\mathcal{C})$.
2) There exists an elementary interval $\prod_{i=1}^n [0, q^{-l_i})$ of volume q^{-k} containing exactly q points and no smaller

elementary intervals of this form containing exactly q points exist.

Corollary 3.4: An $[nr, k, d]$ NMDS code $\mathcal{C}$ in the ordered Hamming space forms a $(k-1, n, r, q)$ OOA of index q. The corresponding distribution $P(\mathcal{C}) \subset U^n$ forms a $(k-r, k, n)$-net for $k-1 \geq r$.

Remark 3.5: Distributions of points in the unit cube obtained from NMDS codes have properties similar to those of distributions obtained from MDS codes. In particular, the points obtained from an $[nr, k, d]$ MDS code in $\mathbb{F}_q^{r,n}$ satisfy part (1) of Theorem 3.3 and give rise to a $(k-r, k, n)$-net for $k \geq r$ [14].

IV. Weight distribution of NMDS codes

Let $\Omega(I)$ be the set of maximal elements of an ideal I and let $\tilde{I} \triangleq I \setminus \Omega(I)$.

Let $\mathcal{C}$ be an NMDS $[n, k, d]$ linear poset code. Let $A_I \triangleq \{x \in \mathcal{C} : \langle \operatorname{supp} x \rangle = I\}$ be the number of codewords with l.a. support exactly I and let $A_s = \sum_{I:|I|=s} A_I$.

Theorem 4.1: The weight distribution of $\mathcal{C}$ has the following form:

$$A_s = \sum_{I \in \mathcal{I}_s} \sum_{l=0}^{s-d-1} (-1)^l \binom{|\Omega(I)|}{l} (q^{s-d-l} - 1) + \\ + (-1)^{s-d} \sum_{I \in \mathcal{I}_s} \sum_{J \in \mathcal{I}_d(I), J \supseteq \tilde{I}} A_J, n \geq s \geq d, \quad (3)$$

where $\mathcal{I}_s \triangleq \{I \subseteq \overrightarrow{\mathcal{P}} : |I| = s\}$, $\mathcal{I}_s(I) \triangleq \{J : J \subseteq I, |J| = s\}$.

PROOF. The computation below is driven by the fact that ideals are fixed by the sets of their maximal elements.

The number of codewords of weight s is given by $A_s = |\cup_{I \in \mathcal{I}_s} \mathcal{C} \cap S_I|$, where $S_I \triangleq \{x \in \mathbb{F}_q^n : \langle \operatorname{supp} x \rangle = I\}$ is the sphere with l.a. support exactly I. The above expression can be written as

$$\Big| \bigcup_{I \in \mathcal{I}_s} \mathcal{C} \cap S_I \Big| = \sum_{I \in \mathcal{I}_s} \Big(|\mathcal{C} \cap B_I^*| - \Big| \bigcup_{J \in \mathcal{I}_{s-1}(I)} \mathcal{C} \cap B_J^* \Big| \Big),$$

where $B_I \triangleq \{x \in \mathbb{F}_q^n : \langle \operatorname{supp} x \rangle_{\overrightarrow{\mathcal{P}}} \subseteq I\}$ and $B_I^* \triangleq B_I \setminus \mathbf{0}$. We determine the cardinality of the last term using the inclusion-exclusion principle.

$$\Big| \bigcup_{J \in \mathcal{I}_{s-1}(I)} \mathcal{C} \cap B_J^* \Big| = \sum_{J \in \mathcal{I}_{s-1}(I)} |\mathcal{C} \cap B_J^*| + \cdots + \\ + (-1)^{|\Omega(I)|-1} \sum_{J_1 \neq \cdots \neq J_{|\Omega(I)|} \in \mathcal{I}_{s-1}(I)} \Big| \mathcal{C} \cap \Big(\bigcap_i B_{J_i}^* \Big) \Big|. \quad (4)$$

Since $\mathcal{C}^\perp$ has minimum distance k, $\mathcal{C}$ forms an orthogonal array of strength $k-1$ with respect to the dual poset $\overleftarrow{\mathcal{P}}$. This provides us with an estimate for each individual term in (4) as described below. For distinct $J_1, \ldots, J_l \in \mathcal{I}_{s-1}(I)$, we let $J \triangleq \cap_{i=1}^l J_i$. Using the fact that J does not contain l maximal elements of I, we get

$$\Big| \Big\{ \{J_1, \ldots, J_l\} : J_i \text{ distinct}, J_i \in \mathcal{I}_{s-1}(I) \Big\} \Big| = \binom{|\Omega(I)|}{l}.$$

For any $s \geq d+1$ consider the complement I^c of an ideal $I \in \mathcal{I}_s$. Since $|I^c| \leq n-d-1 = k-1$, the code $\mathcal{C}$ supports an orthogonal array of strength $n-s$ and index q^{s-d} in the coordinates defined by I^c. Since $\cap_{i=1}^l B_{J_i}^* = B_J^*$ and since B_J^* does not contain the $\mathbf{0}$ vector, we obtain

$$\Big| \mathcal{C} \cap \Big(\bigcap_{i=1}^l B_{J_i}^* \Big) \Big| = q^{s-d-l} - 1, \quad 1 \leq l \leq s-d-1.$$

Finally, for $l = s-d$ we obtain $|\mathcal{C} \cap (\cap_{i=1}^l B_{J_i}^*)| = A_J$. Thus

$$\Big| \bigcup_{J \in \mathcal{I}_{s-1}(I)} \mathcal{C} \cap B_J^* \Big| = \sum_{l=1}^{s-d-1} (-1)^{l-1} \binom{|\Omega(I)|}{l} (q^{s-d-l} - 1) + \\ + \sum_{J \in \mathcal{I}_d(I), J \supseteq \tilde{I}} (-1)^{s-d-1} A_J. \quad \blacksquare$$

As a corollary of the above theorem, we obtain the weight distribution of NMDS codes in the ordered Hamming space $\mathbb{F}_q^{r,n}$. By definition, the number of vectors of ordered weight s in a code $\mathcal{C} \in \mathbb{F}_q^{r,n}$ equals $A_s = \sum_{e:|e|'=s} A_e$, where A_e is the number of codevectors of shape e.

Corollary 4.2: The weight distribution of an ordered NMDS code $\mathcal{C} \in \mathbb{F}_q^{r,n}$ is given by

$$A_s = \sum_{l=0}^{s-d-1} (-1)^l \left(\sum_{e:|e|'=s} \binom{|e|}{l} \binom{n}{e_0, \ldots, e_r} \right) (q^{s-d-l} - 1) \\ + (-1)^{s-d} \sum_{e:|e|'=d} N_s(e) A_e, \quad s = d, d+1, \ldots, n, \quad (5)$$

where

$$N_s(e) \triangleq \sum_{f:|f|'=s} \binom{e_{r-1}}{f_r - e_r} \binom{e_{r-2}}{(f_r + f_{r-1}) - (e_r + e_{r-1})} \times \\ \cdots \times \binom{e_0}{|f| - |e|}.$$

Proof: Recall that the shape of an ideal I is $\operatorname{shape}(I) = e = (e_1, \ldots, e_r)$, where $e_j, j = 1, \ldots, r$ is the number of chains of length j contained in I. We obtain $|\Omega(I)| = |e|$ and

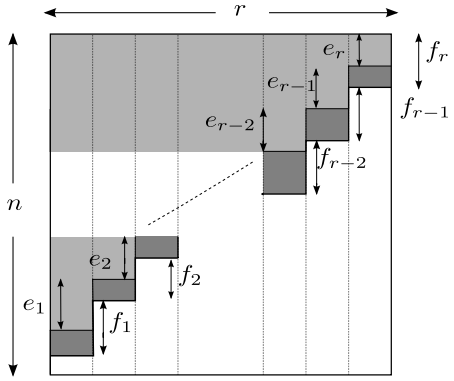
$$\sum_{I \in \mathcal{I}_s} \binom{|\Omega(I)|}{l} = \sum_{e:|e|'=s} \binom{|e|}{l} \binom{n}{e_0, \ldots, e_r}.$$

To determine the last term in (3), we rewrite it as

$$\sum_{I \in \mathcal{I}_s} \sum_{J \in \mathcal{I}_d(I), J \supseteq \tilde{I}} A_J = \sum_{J \in \mathcal{I}_d} |\{I \in \mathcal{I}_s : \tilde{I} \subseteq J \subseteq I\}| A_J \\ = \sum_{e:|e|'=d} N_s(e) \sum_{J:\operatorname{shape}(J)=e} A_J,$$

where $N_s(e) = |\{I \in \mathcal{I}_s : \tilde{I} \subseteq J \subseteq I, J \text{ fixed}, \operatorname{shape}(J) = e\}|$.

Clearly, $\sum_{J:\operatorname{shape}(J)=e} A_J = A_e$. To determine $N_s(e)$ let J be an ideal as shown in Fig. 1. The ideals I which satisfy the constraints in the set defined by $N_s(e)$ have the form as shown in Fig. 1. Letting $f = \operatorname{shape}(I)$, we note that the components of the shape f must satisfy $f_r \geq e_r$, $f_r + f_{r-1} \geq e_r + e_{r-1} \geq$



Light gray region: ideal J of shape e.
Light gray + Dark gray region: ideal I of shape f.

Fig. 1. To the proof of Corollary 4.2

$f_r, \ldots, f_1 + \cdots + f_r = |f| \geq |e| = e_1 + \cdots + e_r \geq f_2 + \cdots + f_s$, and $|f|' = s$. It is now readily seen that $N_s(e)$ is as stated in Cor. 4.2. ∎

Remark: For $r = 1$ we obtain $|e| = |e|' = e_1 = d, |f| = f_1 = s$ and $N_s(e) = \binom{n-d}{s-d}$. Thus one can recover the expression for the weight distribution of an NMDS code in Hamming space as stated in [4].

Unlike the case of poset MDS codes [7], the weight distribution of NMDS codes is not completely known until we know the number of codewords with l.a. support J for every ideal of weight J of size d. In particular, for NMDS codes in the ordered Hamming space we need to know the number of codewords of every shape e with $|e|' = d$. This highlights the fact that the combinatorics of codes in the poset space (ordered space) is driven by ideals (shapes) and their support sizes, and that the weight distribution is a derivative invariant of those more fundamental quantities.

V. Constructions of NMDS codes

In this section we present some simple constructions of NMDS codes in the ordered Hamming space for the cases $n = 1, 2$. We are not aware of any general code family of NMDS codes for larger n.

n=1: For $n = 1$ the construction is quite immediate once we recognize that an NMDS $[r, k, d]$ code is also an OOA of r.a. strength $k - 1$ and index q. Let I_l denote the identity matrix of size l. Let $x = (x_1, \ldots, x_r)$ be any vector of l.a. weight $d = r - k$, i.e. $x_d \neq 0$ and $x_l = 0$, $l = d + 1, \ldots, r$. Then the following matrix of size $k \times r$ generates an NMDS code with the above parameters

$$\begin{bmatrix} x_1 \ldots x_d & 0 & \mathbf{0} \\ M & \mathbf{0} & I_{k-1} \end{bmatrix}, \tag{6}$$

where the $\mathbf{0}$s are zero vectors (matrices) of appropriate dimensions and $M \in \mathbb{F}_q^{(k-1)\times d}$ is any arbitrary matrix.

n=2: Let $D_l = \begin{bmatrix} 0 & \ldots & 1 \\ \vdots & \iddots & \vdots \\ 1 & \ldots & 0 \end{bmatrix}$ be the $l \times l$ matrix with 1 along the inverse diagonal and 0 elsewhere. Let u and v be two vectors of length r in $\mathbb{F}_q^{r,1}$ and l.a. weights $r - k_1$ and $r - k_2$ respectively and let $K = k_1 + k_2$. The following two matrices correspond to the two blocks of the generator matrix of a $[2r, K, 2r - K]$ linear NMDS code in $\mathbb{F}_q^{r,2}$.

$$\begin{bmatrix} u_1 \ldots u_{r-k_1-1} & u_{r-k_1} & 0 & \mathbf{0} \\ \mathbf{0} & 0 & 1 & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & I_{k_1-1} \\ E_r(k_2, k_1) & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix},$$

$$\begin{bmatrix} v_1 \ldots v_{r-k_2-1} & v_{r-k_2} & 0 & \mathbf{0} \\ \mathbf{0} & 0 & 1 & 0 \\ E_r(k_1, k_2) & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & I_{k_2-1} \end{bmatrix},$$

where $E_r(i, j)$ is an $(i-1) \times (r-j-1)$ matrix given by:

$$E_r(i,j) = \begin{cases} \begin{bmatrix} D_{r-j-1} \\ \hline \mathbf{0}_{(i+j-r)\times(r-j-1)} \end{bmatrix}, & i + j > r, \\ \\ \left[\begin{array}{c|c} \mathbf{0}_{(i-1)\times(r-i-j)} & D_{i-1} \end{array} \right], & i + j \leq r. \end{cases}$$

From the form of the generator matrix it can be seen that any $K - 1$ r.a. columns of the above matrix are linearly independent. But the last k_1 and k_2 columns from the first and the second blocks respectively are linearly dependent. This implies that it forms an OOA of r.a. strength exactly $K - 1$. Hence the dual of the code has distance K. Finally, the minimum weight of any vector produced by this generator matrix is $2r - K$. Hence by Lemma 2.4, this matrix generates an NMDS code.

References

[1] A. Barg and P. Purkayastha, *Bounds on ordered codes and orthogonal arrays*, Moscow Math. Journal **9** (2009), no. 2, 211–243.

[2] R. A. Brualdi, J.S. Graves, and K. M. Lawrence, *Codes with a poset metric*, Discrete Math. **147** (1995), no. 1-3, 57–72.

[3] M. de Boer, *Almost MDS codes*, Des. Codes Crypt. **9** (1996), 143–155.

[4] S. Dodunekov and I. Landgev, *Near-MDS codes*, J. of Geometry **54** (1995), no. 1, 30–43.

[5] S. T. Dougherty and M. M. Skriganov, *Maximum distance separable codes in the ρ metric over arbitrary alphabets*, Journal of Algebraic Combinatorics **16** (2002), 71–81.

[6] A. Faldum and W. Willems, *A characterization of MMD codes*, IEEE Trans. Inform. Theory **44** (1998), no. 4, 1555–1558.

[7] J. Y. Hyun and H. K. Kim, *Maximum distance separable poset codes*, Des. Codes Cryptogr. **28** (2008), no. 3, 247–261.

[8] K. M. Lawrence, *A combinatorial characterization of (t, m, s)-nets in base b*, J. Combin. Designs **4** (1996), 275–293.

[9] W. J. Martin and D. R. Stinson, *Association schemes for ordered orthogonal arrays and (T, M, S)-nets*, Canad. J. Math. **51** (1999), no. 2, 326–346.

[10] G. L. Mullen and W. Ch. Schmid, *An equivalence between (t, m, s)-nets and strongly orthogonal hypercubes*, Journal of Combin. Theory, Ser. A **76** (1996), 164–174.

[11] H. Niederreiter, *Low-discrepancy point sets*, Monatsh. Math. **102** (1986), no. 2, 155–167.

[12] M. Yu. Rosenbloom and M. A. Tsfasman, *Codes for the m-metric*, Problems of Information Transmission **33** (1997), no. 1, 45–52.

[13] R. Roth, *Introduction to coding theory*, Cambridge University Press, Cambridge, 2006.

[14] M. M. Skriganov, *Coding theory and uniform distributions*, Algebra i Analiz **13** (2001), no. 2, 191–239, English translation in St. Petersburg Math. J. **13** (2002), no. 2, 301–337.

[15] M. M. Skriganov, *On linear codes with large weights simultaneously for the Rosenbloom-Tsfasman and Hamming metrics*, J. of Complexity **23** (2007), 926–936

[16] V. Wei, *Generalized Hamming weights for linear codes*, IEEE Trans. Inform. Theory **37** (1991), no. 5, 1412–1418.