Journal of Algebraic Combinatorics **16** (2002), 71–81

Maximum Distance Separable Codes in the ρ Metric over Arbitrary Alphabets

STEVEN T. DOUGHERTY* doughertys1@uofs.edu
Department of Mathematics, University of Scranton, Scranton, PA 18510, USA

MAXIM M. SKRIGANOV† skrig@pdmi.ras.ru
Steklov Institute of Mathematics at St. Petersburg, Fontanka 27, St. Petersburg 191011, Russia

Received August 7, 2000; Revised September 21, 2001

Abstract. We give a bound for codes over an arbitrary alphabet in a non-Hamming metric and define MDS codes as codes meeting this bound. We show that MDS codes are precisely those codes that are uniformly distributed and show that their weight enumerators based on this metric are uniquely determined.

Keywords: MDS codes, uniform distributions

1. Introduction

In a classical coding setting, codes are subsets of the ambient space $\mathbb{F}_q^n$ and are investigated with relation to the Hamming metric. Recently, in [5] and [6] the space of $Mat_{n,s}(\mathbb{F}_q)$, the ambient space of n by s matrices with entries from $\mathbb{F}_q$, was studied and bounds were given for the minimum weight with respect to a non-Hamming metric and MDS codes in this space were defined, with respect to this metric. In a different setting some of these ideas were also investigated in [4], namely in terms of orthogonal arrays and association schemes. In [2], MacWilliams relations for codes in these spaces for the naturally defined weight enumerators were given.

In this paper we work in the ambient space of n by s matrices with entries from a finite alphabet $\mathcal{A}$. We generalize the bound given in [5], which is similar to the Singleton bound, and examine the relationship between these codes and show that the codes meeting this bound are precisely the codes that are distributed uniformly with respect to this metric.

1.1. Definitions and notations

Let $\mathcal{A} = \{a_1, \ldots, a_q\}$ be any finite alphabet and $Mat_{n,s}(\mathcal{A})$ denote the set of all matrices with n rows and s columns with entries from $\mathcal{A}$. A code is a subset of $Mat_{n,s}(\mathcal{A})$.

*The author thanks the Euler and Steklov Institutes in St. Petersburg, Russia, where he stayed while most of this work was done.
†The author was partially supported by the Russian fund for Fundamental Research (Project No. 99-01-00106) and by INTAS (Grant No. 00-429).

Note that since we are assuming no binary operations in $\mathcal{A}$, we do not define a linear code.

If $\omega, \omega' \in Mat_{1,s}(\mathcal{A})$ with $\omega = (\alpha_1, \ldots, \alpha_s)$ and $\omega' = (\beta_1, \ldots, \beta_s)$ then we define the metric ρ by $\rho(\omega, \omega') = \max\{i \mid \alpha_i \neq \beta_i\}$, and $\rho(\omega, \omega') = 0$ if $\omega = \omega'$. For $\Omega, \Omega' \in Mat_{n,s}(\mathcal{A})$ define

$$\rho(\Omega, \Omega') = \sum_{j=1}^{n} \rho(\omega_j, \omega'_j)$$

where ω_j, ω'_j are the j-th rows of Ω and Ω' respectively. Certainly, the fact that the elements are matrices is not critical to the definition of the metric. An equivalent definition can easily be made for a vector in $\mathcal{A}^{ns}$, simply separate the coordinates into n groups of s coordinates. Possible information theoretic applications of this metric are described in [5].

For vectors in $Mat_{1,s}(\mathcal{A})$ we not only have the triangle inequality, but more importantly we have the stronger bound:

$$\rho(\omega, \omega') \leq \max\{\rho(x, \omega), \rho(x, \omega')\} \leq \rho(x, \omega) + \rho(x, \omega') \tag{1}$$

The minimum distance of a code C is given by

$$\rho(C) = \min\{\rho(\Omega, \Omega') \mid \Omega, \Omega' \in C,\ \Omega \neq \Omega'\}.$$

Given a code $C \subset Mat_{n,s}(\mathcal{A})$. The following set of ns non-negative integers

$$w_r(\Omega') = w_r(C; \Omega') = |\{\Omega \in C : \rho(\Omega, \Omega') = r\}|, \quad r \in \mathbb{N}_0, \quad 0 \leq r \leq ns \tag{2}$$

is called the *weight spectrum* of the code C relative to an element $\Omega' \in C$. We write $|E|$ for the cardinality of a subset $E \subset Mat_{n,s}(\mathcal{A})$.

The weight spectrum gives the number of elements of a code with a given ρ distance from a specific point of reference, Ω'. From a coding perspective [5] and from the corresponding notion in uniform distributions [6], we want these elements to be as far apart from each other as possible, with respect to the metric ρ, i.e. we want the smallest ρ distance between any two elements to be as large as possible. As with codes in the classical setting we also want the code to be as large as possible. These are, of course, conflicting aims. Hence, what is sought is the largest number of elements one can have and maintain a large minimum distance, or similarly, to find the greatest possible minimum distance for a given number of elements.

In [6], it is shown that every code $C \subset Mat_{n,s}(\mathbb{F}_q)$ with q^k elements satisfies the bound $\rho(C) \leq ns - k + 1$. Codes meeting this bound were called Maximum Distance Separable codes. In [5], it was proven that for a code $C \in Mat_{n,s}(\mathbb{F}_q)$ with cardinality K with minimum distance d, $K \leq q^{ns-d+1}$. The proof of this theorem generalizes directly to the following case:

Theorem 1.1 *Let $\mathcal{A}$ be any finite alphabet with q elements and let $C \subset Mat_{n,s}(\mathcal{A})$, be an arbitrary code, then*

$$|C| \leq q^{ns-d+1}. \tag{3}$$

Proof: The proof follows exactly as the proof given in [5]. Namely, mark the first $d-1$ positions lexicographically. Two elements of C never coincide in all other positions since otherwise the distance between them would be less than d. Hence $|C| \leq q^{ns-d+1}$. □

Note that this result resembles the well known bound for the Hamming metric ([3], Chapter 11).

Corollary 1.2 *Let $C \subset Mat_{n,s}(\mathcal{A})$, where $|\mathcal{A}| = q$, be an arbitrary code consisting of q^k, $0 \leq k \leq ns$, points. Then*

$$\rho(C) \leq ns - k + 1. \tag{4}$$

Naturally, we define a code meeting this bound as a *Maximum Distance Separable Code with respect to the ρ metric* (or simply MDS codes for short). This does not cause confusion with the standard definition of MDS codes since an MDS code with respect to the Hamming metric is simply an MDS code with respect to the ρ metric with $s = 1$.

2. Uniformly distributed codes

Throughout this section, C is a code with q^k elements.

For a given $A = (a_1, \ldots, a_n)$, with $0 \leq a_j \leq s$, define an elementary box centered at $\Omega \in Mat_{n,s}(\mathcal{A})$ by

$$V_A(\Omega) = \{\Omega' \mid \rho(\omega_i, \omega_i') \leq a_i,\ A = (a_1, \ldots, a_n)\}. \tag{5}$$

We shall define the volume of a box $V_A(\Omega)$ by

$$Vol(V_A(\Omega)) = \frac{|V_A(\Omega)|}{|Mat_{n,s}(\mathcal{A})|} = \frac{q^{a_1+\cdots+a_n}}{q^{ns}} = q^{(a_1+\cdots+a_n)-ns}, \tag{6}$$

so that $Vol(Mat_{n,s}(\mathcal{A})) = 1$.

Let F_k be the family of elementary boxes with volume q^{-k}. We say that a code with q^k elements, is *Uniformly Distributed* (abbreviated UD) if each elementary box of F_k intersects the code in exactly one point.

In [6], it is shown that MDS codes in $Mat_{n,s}(\mathbb{F}_q)$ are intimately related to uniform distributions in the unit n-dimensional cube, $[0, 1)^n$. The present situation is similar, namely we have the following theorem.

Theorem 2.1 *A code C with q^k elements is an MDS code if and only if it is Uniformly Distributed.*

To prove this theorem we require two lemmas.

Lemma 2.2 *Two given points $X, X' \in Mat_{n,s}(\mathcal{A})$ fall simultaneously into an elementary box belonging to the family F_k if and only if $\rho(X, X') \leq ns - k$.*

Proof: If $\rho(X, X') \leq ns - k$ then take $V_A(X)$ with $a_i = \rho(x_i, x_i')$ and then we have that $X' \in V_A(X)$, by the choice of the a_i.

Next assume $X, X' \in V_A(\Omega)$ for some $\Omega \in Mat_{n,s}(\mathcal{A})$ and $A = (a_1, \ldots, a_n)$ with $Vol(V_A(\Omega)) = q^{-k}$, which implies that $\sum a_i = ns - k$, then $\rho(x_i, x_i') \leq \max\{\rho(x_i, \omega_i), \rho(x_i', \omega_i)\} \leq a_i$, giving that $\rho(X, X') \leq ns - k$. □

Lemma 2.3 *Two elementary boxes, $V_A(\Omega)$ and $V_A(\Omega')$, with the same A, either coincide or are disjoint. Therefore, $Mat_{n,s}(\mathcal{A})$ can be partitioned by elementary boxes with a given A.*

Proof: Consider two elementary boxes $V_A(\Omega)$ and $V_A(\Omega')$. Assume the boxes are not disjoint. Then there exists a point $X \in V_A(\Omega) \cap V_A(\Omega')$ which implies

$$\rho(x_i, \omega_i) \leq a_i \quad \text{and} \quad \rho(x_i, \omega_i') \leq a_i$$

for $i = 1, \ldots, n$.

By (1), it is clear that $\rho(\omega_i, \omega_i') \leq \max\{\rho(x_i, \omega_i), \rho(x_i, \omega_i')\}$. This gives that $\Omega \in V_A(\Omega')$ and $\Omega' \in V_A(\Omega)$.

If $Y \in V_A(\Omega)$ then $\rho(y_i, \omega_i) \leq a_i$ for all i. Since $\rho(\omega_i', \omega_i) \leq a_i$ for all i and $\rho(y_i, \omega_i') \leq \max\{\rho(y_i, \omega_i), \rho(\omega_i, \omega_i')\}$ we have that $Y \in V_A(\Omega')$. Hence the two boxes are equal. □

Remark In general, this lemma is not true for boxes of a fixed volume, but only when A is fixed.

Proof of Theorem 2.1: Let C be an MDS code then, by definition, $\rho(C) = ns - k + 1$. By Lemma 2.3, $Mat_{n,s}(\mathcal{A})$ can be partitioned by elementary boxes $V_A(\Omega)$. The number of such boxes in the partition is obviously equal to q^{ns-k}. Therefore each box $V_A(\Omega)$ contains exactly one point of C. Hence C is uniformly distributed.

Let C be a UD code, then by definition each elementary box $V_A(\Omega) \in F_k$ contains exactly one point of C. Therefore, for any two distinct points $x, x' \in C$ we have $\rho(x, x') > ns - k$ by Lemma 2.2. Hence $\rho(x, x') \geq ns - k + 1$, and C is an MDS code. □

For a fixed $A = (a_1, \ldots, a_n)$, the elementary boxes V_A partition the ambient space by Lemma 2.3. If C is an MDS code then each box contains a single point. Note that this is similar to a perfect code, except that the spheres are replaced by elementary boxes with a fixed A.

3. Weight enumerators

In [6], a version of the following theorem is proven for codes in $Mat_{n,s}(\mathbb{F}_q)$. We shall extend the result to codes in $Mat_{n,s}(\mathcal{A})$. By showing that the weight spectrum is determined for codes over an arbitrary alphabet, we show that this determination results from a purely combinatorial argument not dependent on an algebraic structure of the underlying alphabet. We shall see that only the inclusion and exclusion principle is used in the proof.

Before stating the next theorem we need an additional definition. We let

$$\sigma_s(l,r) = \left|\left\{A = (a_1, a_2, \ldots, a_l) \in \mathbb{N}^l \;\middle|\; \sum a_i = r,\ 0 < a_j \le s,\ 1 \le j \le l\right\}\right|. \quad (7)$$

Theorem 3.1 *Let C be a Uniformly Distributed (and hence MDS) code in $Mat_{n,s}(\mathcal{A})$ then weights (2) are independent of elements $\Omega' \in C$ and $w_r = w_r(\Omega') = w_r(X')$ are given by*

$$w_0 = 1, \quad w_r = 0 \quad (8)$$

for $0 \le r < \rho(C) = (n-k)s + 1$, and

$$w_r = \sum_{l=1}^{n} \binom{n}{l} \sigma_s(l,r) \sum_{t=0}^{r-\rho(C)} (-1)^t \binom{l}{t} \left(q^{r-\rho(C)+1-t} - 1\right) \quad (9)$$

$$= (q-1) \sum_{l=1}^{n} \binom{n}{l} \sigma_s(l,r) \sum_{t=0}^{r-\rho(C)} (-1)^t \binom{l-1}{t} q^{r-\rho(C)-t} \quad (10)$$

for $\rho(C) \le t \le ns$.

If the alphabet coincides with a finite field then formulas in the above theorem were found in [6], moreover for the case of $s = 1$ (the Hamming metric) this result is well known [3].

We shall require a few definitions and lemmas before proving the theorem. We shall adopt the notation given in [2].

Balls and spheres in the metric ρ were defined in ([6], Section 3) and [5] in the space $Mat_{n,s}(\mathbb{F}_q)$ and later used in [2]. We extend their definition to the present case defining them as follows:

$$B^{(n,s)}(r) = \{\Omega \in Mat_{n,s}(\mathcal{A}) \mid \rho(\Omega) \le r\} \quad (11)$$

$$S^{(n,s)}(r) = \{\Omega \in Mat_{n,s}(\mathcal{A}) \mid \rho(\Omega) = r\} \quad (12)$$

We require the following lemma which was proven in a different setting (with different notation) in [6].

Lemma 3.2 *Each ball is a union of the following subsets*

$$B^{(n,s)}(r) = \bigcup_{r_1+\cdots+r_n=r} V_R \quad (13)$$

where $R = (r_1, \ldots, r_n)$ and $V_R = \{\Omega \mid \rho(\omega_i) \le r_i\}$, and each sphere is the union of the following subsets

$$S^{n,s}(r) = \bigcup_{r_1+\cdots+r_n=r} F_R \quad (14)$$

where $R = (r_1, \ldots, r_n)$ and $F_R = \{\Omega \mid \rho(\omega_i) = r_i\}$.

The following lemma is similar to Lemma 1.2 in [6]. However, it does not follow from the results in [6], because now $\mathcal{A}$ is an arbitrary alphabet, so we include a new proof.

Lemma 3.3 *Let C be an MDS code (equivalently a UD code) with q^k elements in $Mat_{n,s}(\mathcal{A})$, with $|\mathcal{A}| = q$. Let $A = (a_1, \ldots, a_n)$ then*
1. *$V_A(\Omega)$ contains $q^{k-a_1-a_2-\cdots-a_n}$ points of C if $a_1 + a_2 + \cdots + a_n \leq k$.*
2. *$V_A(\Omega)$ contains at most one point of C if $a_1 + a_2 + \cdots + a_n > k$.*

Proof: (1) Let $c_1 + c_2 + \cdots + c_n = k - \sum a_i$, with $b_j = a_j + c_j$ (so that $\sum b_j = k$).

We shall show that $V_A(\Omega)$ is the disjoint union of $q^{c_1+c_2+\cdots+c_n}$ elementary boxes of volume q^{-k}. Since the code is UD each box contains exactly one element so the union contains $q^{c_1+\cdots+c_n} = q^{k-a_1-\cdots-a_n}$ points.

Let $B = (b_1, \ldots, b_n)$ then

$$V_A(\Omega) = \bigcup_{\beta=1}^{c_1+\cdots+c_n} V_B(\Omega_\beta) \tag{15}$$

then $V_A(\Omega)$ is the disjoint union of elementary boxes. We know that the $V_B(\Omega_\beta)$ are either disjoint or coincide by Lemma 2.3. They have to fill the space so there are $\sum c_i$ of these boxes.

(2) We know that if $\sum a_i > k$ then it is contained in an elementary box of volume q^{-k} so it either has 0 or 1 point in the box. □

Proof of Theorem 3.1: Let C be a uniformly distributed (and hence MDS) code with q^k elements, and fix a point Ω'. It is clear that $w_0(\Omega') = 1$, namely Ω' is the only point ρ distance 0 from Ω'.

For $0 \leq r < \rho(C) = ns - k + 1$, we have $w_r(\Omega') = 0$ since $ns - k + 1$ is the minimum ρ distance of the code.

We consider ρ weights $r \geq ns - k + 1$.

By Lemma 3.2 we know that each sphere is a disjoint union of the fragments

$$S^{n,s}(r) = \bigcup_{r_1+\cdots+r_n=r} F_R \tag{16}$$

where $R = (r_1, \ldots, r_n)$.

Consider the fragment F_R, $R = (r_1, \ldots, r_n)$, where l of the r_i are non-zero, we note that $l > 0$ since $r > 0$. We let J denote the set of indices that are non-zero, i.e. $r_i \neq 0$ if and only if $i \in J$. Then we have:

$$F_R = V_{P_0}(\Omega') - \bigcup_{i \in J} V_{P_1}(\Omega') \tag{17}$$

where

$$(P_0)_i = s - r_j \quad 1 \leq j \leq n \tag{18}$$

and

$$(P_i)_j = \begin{cases} s & \text{if } j \notin J \\ s - r_j & \text{if } j \in J \text{ and } j \neq i \\ s - r_j + 1 & \text{if } j \in J \text{ and } j = i. \end{cases} \tag{19}$$

Then

$$(P_0)_1 + \cdots + (P_0)_n = ns - \sum r_i = ns - r. \tag{20}$$

Let $I = \{i_1, \ldots, i_t\} \subset J = \{J_1, \ldots, j_l\}$. Namely, we pick I to be any subset of the non-zero entries of R.

Then we have

$$V_{A_{i_1}}(\Omega') \cap \cdots \cap V_{A_{i_t}}(\Omega') = V_{A_I}(\Omega') \tag{21}$$

where $A_I = (a_1^I, \ldots, a_n^I)$ with

$$a_j^I = \max\{a_j^{i_1}, \ldots, a_j^{i_t}\} = \begin{cases} s - r_j & j \in I \\ s - r_j + 1 & j \in I. \end{cases} \tag{22}$$

Notice that the following relation holds

$$a_1^I + \cdots + a_n^I = ns - r + l. \tag{23}$$

Now we apply the principle of inclusion and exclusion to count $C \cap F_R$, i.e.

$$|C \cap F_R| = |C \cap V - A_0(\Omega')| - \sum_{t=1}^{l} \sum_{I \subset J} (-1)^t \left|C \cap V_{A_I}(\Omega')\right| \tag{24}$$

where the inner sum is taken over all subsets I of J with cardinality t, which consists of $\binom{l}{t}$ summands.

We have

$$|C \cap V_A(\Omega)| = \begin{cases} q^{s - a_1 - \cdots - a_n} & \text{if } \sum a_i < k \\ 1 & \text{if } \sum a_i \geq k \end{cases} \tag{25}$$

which follows from Lemma 3.3.

Putting (25) into (24) and using the previous computations we get

$$\begin{aligned} |C \cap F_r| &= \sum_{t=0}^{r-ns-k-1} (-1)^t \binom{l}{t} q^{r-ns-k-t} + \sum_{t=r-ns-k}^{l} (-1)^t \binom{l}{t} \\ &= \sum_{t=0}^{r-\rho(C)} (-1)^t \binom{l}{t} \left(q^{r-\rho(C)+1-t} - 1\right) \\ &= (q-1) \sum_{t=0}^{r-\rho(C)} (-1)^t \binom{l-1}{t} q^{r-\rho(C)-t}. \end{aligned}$$

Hence the relation is written as

$$w_r = \sum_{l=1}^{n} \sum_{R, H(R)=l} |C \cap F_R| \tag{26}$$

where the inner sum is over all F_R with the Hamming weight of R equal to l. The number of such F_R is $\binom{l}{t}\sigma_s(l, r)$. □

As a corollary to the theorem we get the standard weight enumerators for MDS codes in the Hamming metric by setting $s = 1$, see [3, 6]. When we set $n = 1$ we get

$$\begin{aligned} w_r &= (q-1)\sum_{l=1}^{1} \binom{1}{l} \sigma_s(l, r) \sum_{t=0}^{r-\rho(C)} (-1)^t \binom{l-1}{t} q^{r-\rho(C)-t} \\ &= (q-1)q^{d-s+r-1}. \end{aligned}$$

This result can be viewed in a different way. Let C be a free linear code in $Mat_{1,s}(\mathbb{Z}_q)$ with $|C| = q^k$, that is the code is a submodule and the free rank is equal to the rank. Moreover, assume that the code is MDS, giving that the minimum ρ weight is $s - k + 1$ and that there are vectors of all ρ weight α, with $s - k + 1 \leq \alpha \leq s$.

Let v be a vector with a 1 in the α-th coordinate and a 0 elsewhere. The vector v is not in $C^{\perp}$ since there are non-zero vectors in C with a 1 in the α-th coordinate. Let C_1 denote the subcode of vectors of C that are orthogonal to v and note that C_1 is codimension 1 in C and contains those vectors that are 0 on the α-th coordinate. The vectors that are non-zero on the coordinates are precisely the set $C - C_1$. Moreover,

$$|C - C_1| = |C| - |C_1| = |C| - \frac{|C|}{q} = \frac{q-1}{q}|C|. \tag{27}$$

Then define C_t from C_{t-1} in an analogous manner. It is clear then that C_t has cardinality $\frac{1}{q}|C_{t-1}|$ and that $|C_k - C_{t-1}| = \frac{q-1}{q}|C_t| = \frac{q-1}{q^t}q^k = (q-1)q^{k-t}$. Then setting $d = s+1-r$, it follows then that the number of the vectors of with ρ weight r is $(q-1)q^{k-s+r-1}$. In terms of classical coding language, the k coordinates containing ρ weights can be considered as the information symbols and the other coordinates as the redundancy. Note that the codes are not MDS with respect to the Hamming weight, but that every code in $Mat_{1,s}(\mathbb{Z}_q)$ is equivalent to an MDS code with respect to the ρ metric. However the above result does not require that the code is linear nor that the underlying alphabet has any algebraic structure at all. But we see that the arbitrary code resembles the linear case in a very fundamental way.

4. Projections

Throughout this section when we say that a code is projected on a subset of coordinates, we shall always mean that it is projected on the upper right hand corner, that is if a code in $Mat_{n,s}(\mathcal{A})$ is projected to $Mat_{n',s'}(\mathcal{A})$ with $n' \leq n$ and $s' \leq s$ then it is projected to the

rows $1, 2, \ldots, n'$ and columns $s - s' + 1, s - s' + 2, \ldots, s$. Let π denote the projection to $Mat_{n',s'}(\mathcal{A})$ where $n's' \geq d$.

Theorem 4.1 *Let $C \subset Mat_{n,s}(\mathcal{A})$ be an MDS code with q^k elements. Suppose that $s' \leq s$, $n' \leq n$, and $s'n' \geq k$. Then the projection of C onto $Mat_{n',s'}(\mathcal{A})$ is an MDS code.*

Before proving the theorem we require a lemma.

Lemma 4.2 *Let C be an MDS code in $Mat_{n,s}(\mathcal{A})$, with q^k elements. Then the code πC has q^k distinct elements, i.e. the projection is injective.*

Proof: First of all, we note that for two arbitrary points $\Omega, \Omega' \in Mat_{n,s}(\mathcal{A})$ we have

$$\rho(\Omega, \Omega') \leq \rho(\pi\Omega, \pi\Omega') + (s - s')n' + s(n - n') = \rho(\pi\Omega, \pi\Omega') + sn - s'n' \quad (28)$$

that follows at once from the definition of the projection π.

Assume Ω and Ω' are two points such that $\pi\Omega = \pi\Omega'$. Then $\rho(\Omega, \Omega') \leq n'(s - s') + (n - n')s = ns - n's' \leq ns - d$, which contradicts that the closest any two points are with respect to the ρ metric is $ns - d + 1$. □

Proof of Theorem 4.1: Let $\Omega \in C$ and denote the i-th row of Ω by ω_i. We shall use $\rho_{n,s}$ and $\rho_{n',s'}$ to denote the ρ metric in the $Mat_{n,s}(\mathcal{A})$ and $Mat_{n',s'}(\mathcal{A})$ respectively.

Notice by Lemma 4.2 the projection is injective, i.e. $|\pi C| = |C|$.

We have

$$\rho_{n,s}(\Omega) = \rho_{1,s}(\omega_1) + \cdots + \rho_{1,s}(\omega_n) \geq ns - d + 1. \quad (29)$$

Case 1: $s = s', \quad n' < n$

$$\begin{aligned}\rho_{n',s}(\pi_{n',s}\Omega) &= \rho_{1,s}(\omega_1) + \cdots + \rho_{1,s}(\omega_{n'}) \\ &= \rho_{1,s}(\omega_1) + \cdots + \rho_{1,s}(\omega_n) - \rho_{1,s}(\omega_{n'+1}) - \cdots - \rho_{1,s}(\omega_n) \\ &\geq ns - d + 1 - s(n - n') = n's - d + 1\end{aligned}$$

Case 2: $s' < s, \quad n' = n$

$$\rho_{n,s'} = \begin{cases} \rho_{1,s}(\omega) - (s - s'), & \text{if } \rho_{1,s} \geq (s - s') \\ 0 = \rho_{1,s}(\omega) - \rho_{1,s}(\omega), & \text{if } \rho_{1,s}(\omega) < (s - s') \end{cases}$$

Without loss of generality, let the second relation be valid to rows $j = 1, \ldots, l$ and the first relation be valid for rows $j = l + 1, \ldots, n$.

Then

$$\begin{aligned}\rho_{s',n}(\pi_{s',n})\Omega = \rho_{1,s}(\omega_1) - \rho_{1,s}(\omega_1) + \cdots + \rho_{1,s}(\omega_l) - \rho_{1,s}(\omega_l) + \rho_{s,1}(\omega_{l+1}) \\ - (s - s') + \cdots + \rho_{s,1}(\omega_n) - (s - s')\end{aligned}$$

$$
\begin{aligned}
&= \rho_{s,n}(\Omega) - \rho_{s,1}(\omega_1) - \cdots - \rho_{s,1}(\omega_l) - (n-l)(s-s') \\
&\geq ns - d + 1 - \rho_{1,s}(\omega_1) - \cdots - \rho_{1,s}(\omega_l) - ns + ns' + ls - ls' \\
&= ns' - d + 1 + l(s-s') - \rho_{1,s}(\omega_1) - \cdots - \rho_{s,1}(\omega_l) \\
&\geq ns' - d + 1
\end{aligned}
$$

because $\rho_{1,s}(\omega_j) \leq s - s'$ for $j = 1, \ldots, l$. □

4.1. Existence of MDS codes over $\mathbb{Z}_q$

In this section, we shall use the Chinese Remainder Theorem to construct MDS codes and show when such codes can exist. Here we shall assume that the codes are linear in $Mat_{n,s}(\mathbb{Z}_q)$, i.e. the codes are submodules of $Mat_{n,s}(\mathbb{Z}_q)$. Let q be any integer greater than 1 with $q = \prod_{i=1}^{\alpha} p_i^{a_i}$, where the p_i are distinct primes, and let C_i be a code in $Mat_{n,s}(\mathbb{Z}_{p_i^{a_i}})$. Let

$$C = CRT(C_1, \ldots, C_\alpha) = \left\{ c \mid c \big(\text{mod } p_i^{a_i}\big) \in C_i \text{ for all } i \right\}.$$

Namely C is the Chinese Remainder Theorem applied coordinatewise on all elements of $C_1 \times C_2 \times \cdots \times C_\alpha$. See [1] for an application of this map to MDS codes over rings in the Hamming metric.

Lemma 4.3 *Let C be constructed as above. Then $|C| = |C_1| \times |C_2| \times \cdots \times |C_\alpha|$ and $\rho(C) \geq \min\{\rho(C_i)\}$.*

Proof: The cardinality follows immediately. If $v \in C$ with $\rho(c) < \rho(C_i)$ for some i then $\rho(v(\text{mod } p_i^{a_i})) < \rho(C_i)$ which is a contradiction unless $v(\text{mod } p_i^{a_i}) = \mathbf{0}$ with $v \neq \mathbf{0}$ which is impossible since *CRT* is an isomorphism. □

Lemma 4.4 *Let $C_1, C_2, \ldots, C_\alpha$ be MDS codes over $\mathbb{Z}_{p_i^{a_i}}$ with $|C_i| = (p_i^{a_i})^k$, then $C = CRT(C_1, \ldots, C_\alpha)$ is an MDS code over $\mathbb{Z}_q$.*

Proof: The previous lemma gives that $|C| = q^k$ and $\rho(C) \geq ns - k + 1$, and by the bound (4) we have $\rho(C) = ns - k + 1$. □

In [6], Theorem 5.1 it is shown that for each $1 \leq k \leq ns$ there exists an MDS code in $Mat_{n,s}(\mathbb{F}_q)$ with q^k elements, if $q \geq n - 1$. This is also shown in [5] as the construction of Reed-Solomon m-codes. However this can easily be made to show that there exists an MDS code in $Mat_{n,s}(\mathbb{Z}_q)$. Namely the code is equivalent to a uniform distribution and this distribution is easily seen to produce an MDS code in $Mat_{n,s}(\mathbb{Z}_q)$. In fact, in many ways, the relationship is more natural in this setting. Hence we have the following:

Theorem 4.5 *There exists MDS codes in $Mat_{n,s}(\mathbb{Z}_q)$ for $q \geq 2$, with $q = \prod p_i^{a_i}$, and $p_i^{a_i} \geq n - 1$, where the p_i are distinct primes, with q^k elements for all k with $1 \leq k \leq ns$.*

Proof: Follows from the above discussion with the previous two lemmas. □

References

1. S.T. Dougherty and K. Shiromoto, "MDR codes over Z_k," *IEEE-IT* **46**(1) (2000), 265–269.
2. S.T. Dougherty and M.M. Skriganov, "MacWilliams duality and the Rosenbloom—Tsfasman metric," *Moscow Mathematical Journal* **2**(1) (2002), 83–99.
3. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.
4. W.J. Martin and D.R. Stinson, "Association schemes for ordered orthogonal arrays and (T, M, S)-nets," *Canad. J. Math.* **51** (1999), 326–346.
5. M. Yu Rosenbloom and M.A. Tsfasman, "Codes for the m-metric," *Problems of Information Transmission*, **33**(1) (1997), 45–52. (Translated from *Problemy Peredachi Informatsii* **33**(1) (1996), 55–63.
6. M.M. Skriganov, "Coding theory and uniform distributions," *Algebra i Analiz* **13**(2) (2001), 191–239. (Translation to appear in *St. Petersburg Math. J.*).