PDMI PREPRINT — 2/2007

# ON LINEAR CODES WITH LARGE WEIGHTS SIMULTANEOULY FOR THE ROSENBLOOM–TSFASMAN AND HAMMING METRICS

**M. M. Skriganov**

Dedicated to Henryk Woźniakowski
on the occasion of his 60th birthday

Steklov Mathematical Institute
at St. Petersburg
Fontanka 27, St. Petersburg 191011
Russia
(E-mail: skrig@pdmi.ras.ru)

January, 2007

ABSTRACT

We show that maximum distance separable codes, or more generally nearly maximum distance separable codes, for the Rosenbloom–Tsfasman metric can meet the Gilbert–Varshamov bound for their Hamming weights. The proof is based on a careful analysis of orbits of a linear group preserving the Rosenbloom–Tsfasman metric.

Supported by RFFI (Project No. 05-01-00935).

## 1. Introduction

A new approach to the theory of uniformly distributed point sets was developed in the recent papers [1, 8, 9]. This approach crucially depends on a specific version of coding theory where, unlike the classical coding theory, two basic metrics should be involved. One of them is the standard Hamming metric while the other one is the Rosenbloom–Tsfasman metric introduced in [7].

In the present paper, we address an aspect of such a version of coding theory. Suppose that a linear code $\mathcal{C} \subset \mathbb{F}_q^\ell$ over a finite field $\mathbb{F}_q$ with a large Rosenbloom–Tsfasman weight $\rho(\mathcal{C})$ is given. What can one say about the Hamming weight $\varkappa(\mathcal{C})$ of this code?

Simple examples show that in general $\varkappa(\mathcal{C})$ is uncontrollable by $\rho(\mathcal{C})$. However, it turns out (see our main Theorem 3.1 in Sec. 3) that if one considers the orbit of the code $\mathcal{C}$ under the action of a linear group preserving the weight $\rho(\mathcal{C})$, then a portion of codes on this orbit have large Hamming weights. Furthermore, if $\mathcal{C}$ is a maximum distance separable (briefly MDS) code, or more generallly *nearly* MDS code, then there exist codes on the orbit of $\mathcal{C}$ which meet the Gilbert–Varshamov bound for their Hamming weights (see Theorem 3.2 below).

We conjecture that point distributions constructed in terms of such specific codes have a series of remarkable properties. The author hopes to consider these intriguing questions in other papers.

The present paper is organized as follows. In Sec. 2, preliminary material on coding theory is collected. Our main Theorem 3.1 is given in Sec. 3. This section also contains asymptotic consequences of Theorem 3.1 given in Theorem 3.2. In sec. 4, we consider the structure of orbits of a group preserving the Rosenbloom–Tsfasman metric, and relying on this consideration, we complete the proof of Theorem 3.1 in Sec. 5.

## 2. Preliminaries

Let $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$ denote the linear space of all matrices with $n$ rows and $s$ columns with entries from a fixed finite field $\mathbb{F}_q$ of $q$ elements. Clearly,

$$\mathrm{Mat}_{n,s}(\mathbb{F}_q) = \prod_{j=1}^{n} \mathrm{Mat}_{1,s}(\mathbb{F}_q) \simeq \mathbb{F}_q^\ell, \quad \ell = ns. \tag{2.1}$$

By definition (cf. [4]), the Hamming weight $\varkappa(\Omega)$, $\Omega \in \mathrm{Mat}_{n,s}(\mathbb{F}_q)$, is equal to the number of nonzero entries of a matrix $\Omega$. In this case, $\varkappa(\Omega_1 - \Omega_2)$ defines the Hamming metric on the space $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$.

The Rosenbloom–Tsfasman weight $\rho(\Omega)$, $\Omega \in \mathrm{Mat}_{n,s}(\mathbb{F}_q)$, is defined as follows. At first, let $n = 1$ and $\omega = (\xi_1, \dots, \xi_s) \in \mathrm{Mat}_{1,s}(\mathbb{F}_q)$. Then, we put $\rho(0) = 0$, and

$$\rho(\omega) = \max\{i : \xi_i \neq 0\} \tag{2.2}$$

for $\omega \neq 0$. Now, let

$$\Omega = (\omega_1, \dots, \omega_n)' = \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} \in \mathrm{Mat}_{n,s}(\mathbb{F}_q), \quad \omega_j \in \mathrm{Mat}_{1,s}(\mathbb{F}_q), \quad 1 \le j \le n.$$

Then, we put

$$\rho(\Omega) = \sum_{j=1}^{n} \rho(\omega_j). \tag{2.3}$$

It is easy to check that $\rho(\Omega) = 0$ if and only if $\Omega = 0$, and that the weights (2.2) and (2.3) satisfy the triangle inequality. Thus, $\rho(\Omega_1 - \Omega_2)$ defines the Rosenbloom–Tsfasman metric on the spase $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$.

Note that definition (2.2) implies even a stronger inequality

$$\rho(\omega_1 - \omega_2) \le \max\{\rho(\omega_1), \rho(\omega_2)\}, \quad \omega_1, \omega_2 \in \mathrm{Mat}_{1,s}(\mathbb{F}_q). \tag{2.4}$$

Thus, the Rosenbloom–Tsfasman metric for $n = 1$ is an ultrametric.

It is obvious that

$$\varkappa(\Omega) \le \rho(\Omega) \le s\varkappa(\Omega), \tag{2.5}$$

and these inequalities cannot be improved on the whole space $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$. Thus, for large $s$ the metric $\rho$ is stronger than $\varkappa$. For $s = 1$ the both metrics coincide.

It is remarkable that fundamental concepts related to the Hamming metric can be very naturally extended to the Rosenbloom–Tsfasman metric (see [2, 7, 8]).

Following [8], we introduce a group $T_s^n$ of linear transformations on $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$ preserving the weight $\rho$. At first, let $n = 1$, $\omega = (\xi_1, \dots, \sigma_s) \in \mathrm{Mat}_{1,s}(\mathbb{F}_q)$, and $T_s$ denote the group of all lower triangular $s$ by $s$ matrices over $\mathbb{F}_q$ with arbitrary nonzero diagonal elements. From definition (2.2), we immediately conclude that the linear mappings

$$t : \mathrm{Mat}_{1,s}(\mathbb{F}_q) \ni \omega \to \omega t \in \mathrm{Mat}_{1,s}(\mathbb{F}_q), \quad t \in T_s, \tag{2.6}$$

preserve the weight $\rho : \rho(\omega t) = \rho(\omega)$.

Now, let $\Omega = (\omega_1, \dots, \omega_n)' \in \mathrm{Mat}_{n,s}(\mathbb{F}_q)$, $\omega_j \in \mathrm{Mat}_{1,s}(\mathbb{F}_q)$, $1 \le j \le n$, and

$$T_s^n = \prod_{j=1}^{n} T_s \tag{2.7}$$

denote the direct product of $n$ copies of $T_s$. Then, the linear mappings

$$\tau : \mathrm{Mat}_{n,s}(\mathbb{F}_q) \ni \Omega = (\omega_1, \dots, \omega_n)' \to \Omega\tau = (\omega_1, t_1 \dots, \omega_n t_n)' \in \mathrm{Mat}_{n,s}(\mathbb{F}_q), \tag{2.8}$$

$$\tau = (t_1, \dots, t_n) \in T_s^n,$$

preserve the weight $\rho : \rho(\Omega\tau) = \rho(\Omega)$.

Obviously, the orders of the groups $T_s$ and $T_s^n$ can be given by

$$\#\{T_s\} = (q-1)^s q^{\frac{s(s-1)}{2}}, \quad \#\{T_s^n\} = (q-1)^{ns} q^{\frac{ns(s-1)}{2}}. \tag{2.9}$$

We write $\#\{\cdot\}$ for the cardinality of a finite set.

Note that the full group of linear transformations preserving the Rosenbloom–Tsfasman weight is a semidirect product of the group $T_s^n$ and the group of all permutations of rows in matrices $\Omega \in \mathrm{Mat}_{n,s}(\mathbb{F}_q)$. This clame was conjectured in [8] and proved in [3]. However, in the present paper we do not use this fact.

Finally, we recall (see [4], for details) that the Hamming ball

$$B_{n,s}(r) = \{\Omega \in \mathrm{Mat}_{n,s}(\mathbb{F}_q) : \varkappa(\Omega) \le r\}, \quad r \ge 0, \tag{2.10}$$

has the "volume"

$$V_q(\ell, r) = \#\{B_{n,s}(r)\} = \sum_{i=0}^{\lfloor r \rfloor} \binom{\ell}{i} (q-1)^i, \tag{2.11}$$

where $\lfloor \cdot \rfloor$ denotes the integer part of a real number, and $\ell$ is given in (2.1).

Furthermore, for each $\lambda \in [0, \frac{q-1}{q}]$, we have the following asymptotics

$$\frac{\log_q V_q(\ell, \lambda^\ell)}{\ell} = \mathcal{H}_q(\lambda) + o(1), \quad \text{as} \quad \ell \to \infty, \tag{2.12}$$

where $\log_q$ denotes the log in base $q$ and $\mathcal{H}_q$ is the $q$-ary entropy function: $\mathcal{H}_q(0) = 0$, and

$$\mathcal{H}_q(\lambda) = \lambda \log_q (q-1) - \lambda \log_q \lambda - (1-\lambda) \log_q (1-\lambda)$$

for $0 < \lambda \le \frac{q-1}{q}$.

Note that $\mathcal{H}_q(\lambda)$ is a continuous monotonic function increasing on the interval $[0, \frac{q-1}{q}]$ from 0 to 1. Therefore, the inverse function $\mathcal{H}_q^-(x)$ is continuous and monotonic on the interval $[0,1]$ increasing from 0 to $\frac{q-1}{q}$.

We have listed the main auxiliary facts. Some additional facts will be given in the next section.

## 3. The main results

A linear code $\mathcal{C}$ is a subspace in $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$. The parameter $\ell = ns$ is called the *length* of a code. We will consider only linear codes $\mathcal{C} \neq \{0\}$.

Introduce the Hamming and Rosenbloom–Tsfasman weights for a linear code $\mathcal{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ by

$$\mathrm{wt}\,(\mathcal{C}) = \min\{\mathrm{wt}\,(\Omega) : \Omega \in \mathcal{C} \setminus \{0\}\}, \tag{3.1}$$

where wt stands for any one of the weights $\varkappa$ or $\rho$.

Obviously, the group $T_s^n$ preserves the weight $\rho$: $\rho(\mathcal{C}\tau) = \rho(\mathcal{C})$, $\tau \in T_s^n$, where $\mathcal{C}\tau = \{\Omega\tau \colon \Omega \in \mathcal{C}\}$.

In view of (3.1) and (2.5), we have

$$\varkappa(\mathcal{C}) \le \rho(\mathcal{C}) \le s\varkappa(\mathcal{C}). \tag{3.2}$$

Thus, if the weight $\varkappa(\mathcal{C})$ is large, the weight $\rho(\mathcal{C})$ is also large automatically. However, as it was saied in the introduction, our concern here is with the opposite situation when the weight $\rho(\mathcal{C})$ is known to be large and we are interested whether the weight $\varkappa(\mathcal{C})$ can be large as well.

Our main result is the following.

**Theorem 3.1.** *Let $\mathcal{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ be an arbitrary linear code. Suppose that the inequality*

$$q^{\rho(\mathcal{C})} \geq q\Big(\frac{q}{q-1}\Big)^n V_q(\ell, d-1) \tag{3.3}$$

*holds for some positive integer $d$.*

*Then, there exists a nonempty subset $\mathcal{G}(\mathcal{C}) \subset T_s^n$ such that the bound*

$$\varkappa(\mathcal{C}\tau) \geq d \tag{3.4}$$

*holds for all transformations $\tau \in \mathcal{G}(\mathcal{C})$.*

*Furthermore, the cardinality of the subset $\mathcal{G}(\mathcal{C})$ satisfies the bound*

$$\frac{\#\{\mathcal{G}(\mathcal{C})\}}{\#\{T_s^n\}} > 1 - q\Big(\frac{q}{q-1}\Big)^n V_q(\ell, d-1) q^{-\rho(\mathcal{C})} \geq 0. \tag{3.5}$$

The proof of Theorem 3.1 will be given in Sec. 5.

Now we wish to derive some asymptotic consequenes of Theorem 3.1.

The both weights $\varkappa(\mathcal{C})$ and $\rho(\mathcal{C})$ (see (3.1)) satisfy the bound

$$\mathrm{wt}\,(\mathcal{C}) \leq \ell - k(\mathcal{C}) + 1, \tag{3.6}$$

where $k(\mathcal{C})$ denotes the dimension of the linear subspace $\mathcal{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$. For the Hamming weight this is the well known Singleton bound (see [4]), and for the Rosenbloom–Tsfasman weight this bound was proved in [7] (see also [1] and [8]).

If for one of the weight $\varkappa(\mathcal{C})$ or $\rho(\mathcal{C})$ we have the equality in (3.6),

$$\mathrm{wt}\,(\mathcal{C}) = \ell - k(\mathcal{C}) + 1, \tag{3.7}$$

then the code $\mathcal{C}$ is called the *maximum distance separable* (briefly MDS) code for the corresponding metric.

Trivial MDS codes of dimensions 1, $\ell - 1$, and $\ell$ can be easily constructed (say, in the latest case $\mathcal{C} = \mathrm{Mat}_{n,s}(\mathbb{F}_q)$).

Nontrivial MDS codes (of dimension $1 < k(\mathcal{C}) < \ell - 1$) for the Rosenbloom–Tsfasman metric and $s \to \infty$ exist if and only if $q \geq n - 1$ (see [8]). The corresponding conditions in the case of the Hamming metric can be found in [4].

Let us write

$$\rho(\mathcal{C}) = \ell - k(\mathcal{C}) + 1 - \delta(\mathcal{C}), \tag{3.8}$$

where a nonnegative parameter $\delta(\mathcal{C})$ is called the *deficiency* of a code $\mathcal{C}$. Thus MDS codes have zero deficiency.

Let an infinite sequence of linear codes $\mathcal{C}_{n,s} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$, $s \to \infty$, be given. The codes $\mathcal{C}_{n,s}$ are called the *nearly MDS codes* for the Rosenbloom–Tsfasman metric if $\delta(\mathcal{C}_{n,s}) = o(\ell)$ as $s \to \infty$.

One can easily construct linear codes $\mathcal{C}_{n,s} \in \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ of deficiency $\delta(\mathcal{C}_{n,s}) = 0(n \log n)$ (see [8]). Obviously, these codes are nearly MDS codes if $\log n = o(s)$ as $s \to \infty$.

With more complicated methods of [5], one can construct codes of deficiency $\delta(\mathcal{C}_{n,s}) = 0(n)$, moreover this bound can not be improved for large $n$. Obviously, such codes are always nearly MDS codes.

Using the dual codes to linear codes $\mathcal{C}_{n,s} \in \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ of dimension $k(\mathcal{C}_{n,s}) = (n-1)s$ and small deficience $\delta(\mathcal{C}_{n,s})$, one obtains very good distriutions of $q^s$ points in the $n$ dimensional unit cube (see [8]). Therefore, in applications to the theory of uniformly distributed point sets the parameter $n$ is usually assumed to be fixed while the parameter $s \to \infty$. The situation when $s$ is fixed and $n \to \infty$ is also of interest for applications but in this case the behavior of the corresponding point distributions turns out to be very specific (see [6]). Note that in the latest case the metrics $\rho$ and $\varkappa$ are equivalent (see (2.5) and (3.2)).

It is convenient to introduce the following characteristics of a code normalized per unit length

$$\widehat{\rho}(\mathcal{C}) = \frac{\rho(\mathcal{C})}{\ell}, \quad \widehat{\varkappa}(\mathcal{C}) = \frac{\varkappa(\mathcal{C})}{\ell}, \quad \widehat{k}(\mathcal{C}) = \frac{k(\mathcal{C})}{\ell}, \quad \widehat{\delta}(\mathcal{C}) = \frac{\delta(\mathcal{C})}{\ell}.$$

In this notation, relation (3.8) for nearly MDS codes can be written in the form

$$\widehat{\rho}(\mathcal{C}_{n,s}) = 1 - \widehat{k}(\mathcal{C}_{n,s}) + \frac{1}{\ell} - \widehat{\delta}(\mathcal{C}_{n,s}) = 1 - \widehat{k}(\mathcal{C}_{n,s}) + o(1) \quad \text{as} \quad s \to \infty. \tag{3.9}$$

Recall that in coding theory the parameter $\widehat{k}(\,\cdot\,)$ is known as the *rate* of a linear code. Obviously, the group $T^n_s$ preserves the rate: $\widehat{k}(\mathcal{C}_{n,s}\tau) = \widehat{k}(\mathcal{C}_{n,s})$, $\tau \in T^n_s$.

With the above remarks, we have the following corollary of Theorem 3.1.

**Theorem 3.2.** *Let $\mathcal{C}_{n,s}$, $s \to \infty$, be an infinite sequence of linear nearly MDS codes for the Rosenbloom–Tsfasman metric. Suppose also that*

$$\rho(\mathcal{C}_{n,s}) \geq n\{1 - \log_q(q-1)\} + 1 \quad \textit{as} \quad s \to \infty. \tag{3.10}$$

*Then, for all sufficiently large $s$, there exist nonempty subsets $\mathcal{G}(\mathcal{C}_{n,s}) \subset T^n_s$ such that the Gilbert–Varshamov bound (cf. [4])*

$$\widehat{\varkappa}(\mathcal{C}_{n,s}\tau) \geq \mathcal{H}^{\leftarrow}_q(1 - \widehat{k}(\mathcal{C}_{n,s})) + o(1), \quad s \to \infty, \tag{3.11}$$

*holds for all transformations $\tau \in \mathcal{G}(\mathcal{C}_{n,s})$.*

*The cardinality of the subsets $\mathcal{G}(\mathcal{C}_{n,s})$ is given by (3.5) with $\mathcal{C} = \mathcal{C}_{n,s}$.*

*Proof.* With the assumption (3.10), we observe that for all sufficiently large $s$, inequality (3.3) holds for $d = 1$, at least.

Let $D_{n,s} \geq 1$ be the maximum positive integer such that inequality (3.3) holds for $\mathcal{C} = \mathcal{C}_{n,s}$. Then

$$q\Big(\frac{q}{q-1}\Big)^n V_q(\ell, D_{n,s}) > q^{\rho(\mathcal{C}_{n,s})} \geq q\Big(\frac{q}{q-1}\Big)^n V_q(\ell, D_{n,s} - 1). \tag{3.12}$$

Let us put

$$\widehat{D}_{n,s} = \frac{D_{n,s}}{\ell}.$$

Using inequalities (3.12) and asymptotics (2.12), we find that

$$\frac{1}{s}\{1 - \log_q(q-1)\} + \frac{1}{\ell} + \mathcal{H}_q(\widehat{D}_{n,s}) + o(1) > \widehat{\rho}(\mathcal{C}_{n,s}) \geq$$
$$\frac{1}{s}\{1 - \log_q(q-1)\} + \frac{1}{\ell} + \mathcal{H}_q\Big(\widehat{D}_{n,s} - \frac{1}{\ell}\Big) + o(1) \quad \text{as} \quad s \to \infty.$$

Therefore,

$$\widehat{\rho}(\mathcal{C}_{n,s}) = \mathcal{H}_q(\widehat{D}_{n,s}) + o(1) \quad \text{as} \quad s \to \infty,$$

and

$$\widehat{D}_{n,s} = \mathcal{H}_q^{\leftarrow}(\widehat{\rho}(\mathcal{C}_{n,s})) + o(1) = \mathcal{H}_q^{\leftarrow}(1 - \widehat{k}(\mathcal{C}_{n,s})) + o(1) \quad \text{as} \quad s \to \infty. \tag{3.13}$$

In these asymptotic calculations we used the fact that both functions $\mathcal{H}_q(\,\cdot\,)$ and $\mathcal{H}_q^{\leftarrow}(\,\cdot\,)$ are continuous.

By Theorem 3.1, for all sufficiently large $s$ there exist nonempty subsets $\mathcal{G}(\mathcal{C}_{n,s}) \subset T_s^n$ such that the bound

$$\widehat{\varkappa}(\mathcal{C}_{n,s}, \tau) \geq \widehat{D}_{n,s} \tag{3.14}$$

holds for all transformations $\tau \in \mathcal{G}(\mathcal{C}_{n,s})$.

Substituting asymptotics (3.13) into relation (3.14), we obtain inequality (3.11).

The proof of Theorem 3.2 is complete. $\square$

## 4. Orbits of the group $T_s^n$ on $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$

First of all, we wish to describe the structure of orbits of the group $T_s^n$ on the space $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$.

Let $n = 1$, then we introduce the following boxes in $\mathrm{Mat}_{1,s}(\mathbb{F}_q)$:

$$\Pi_a = \{\omega \in \mathrm{Mat}_{1,s}(\mathbb{F}_q) : \rho(\omega) = a\}, \quad a \in Q_s, \tag{4.1}$$

where $Q_s = \{0, 1, \ldots, s\}$. For arbitrary $n$ we put

$$\Pi_A = \prod_{j=1}^{n} \Pi_{a_j} = \{\Omega = (\omega_1, \ldots, \omega_n)' \in \mathrm{Mat}_{n,s}(\mathbb{F}_q) : \rho(\omega_j) = a_j, \quad 1 \leq j \leq n\}, \tag{4.2}$$

where $A = (a_1, \ldots, a_n) \in Q_s^n = \prod_{j=1}^{n} Q_s$.

Obviously, $\Pi_{A_1} \cap \Pi_{A_2} = \varnothing$ if $A_1 \neq A_2$, and the space $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$ can be represented as a disjoint union of all $\Pi_A$, $A \in Q_s^n$:

$$\mathrm{Mat}_{n,s}(\mathbb{F}_q) = \bigcup_{A \in Q_s^n} \Pi_A. \tag{4.3}$$

The following Lemma 4.1 is an improvement of Proposition 2.2(i) of [2].

**Lemma 4.1.** (i) *The orbits of the group $T_s^n$ on $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$ coincide with the boxes $\Pi_A$, $A \in Q_s^n$.*

(ii) *The cardinality of the boxes $\Pi_A$, $A \in Q_s^n$, is given by*

$$\#\{\Pi_A\} = (q-1)^{\varkappa(A)} q^{a_1 + \cdots + a_n - \varkappa(A)}, \tag{4.4}$$

*where $\varkappa(A)$ denotes the "Hamming weight" of the integer vector $A = (a_1, \ldots, a_n)$, that is the number of nonzero entries of $A$.*

(iii) *The stabilizer* $S(\Omega_A)=\{\tau\in T_s^n:\Omega_A\tau=\Omega_A\}$ *of a point* $\Omega_A\in\Pi_A$ *is a subgroup in* $T_s^n$ *of order*

$$\#\{S(\Omega_A)\}=\frac{\#\{T_s^n\}}{\#\{\Pi_A\}}=(q-1)^{ns-\varkappa(A)}q^{\frac{ns(s-1)}{2}-a_1\ldots-a_n+\varkappa(A)}. \tag{4.5}$$

*Proof.* (i) At first, let $n=1$. Then, $\Pi_0=\{0\}$ and the statement is trivial. If $a\geq 1$, then the box $\Pi_a$ consists of all rows $\omega=(\xi_1,\ldots,\xi_s)$ with $\xi_j=0$ for $j>a$, arbitrary $\xi_j\in\mathbb{F}_q$ for $j<a$ and with arbitrary $\xi_a\in\mathbb{F}_q^*=\mathbb{F}_q\setminus\{0\}$. Write $\omega_a=(\xi_{1,a},\ldots,\xi_{s,a})$ with $\xi_{j,a}=\delta_{j,a}$, where $\delta_{j,a}$ is the Kronecker symbol. For a lower triangular matrix $t=(t_{j,i})\in T_s$, $t_{j,i}=0$ for $j>i$, we have $\omega_a t=(t_{1,a},\ldots,t_{s,a})\in\Pi_a$. Thus, $\Pi_a=\{\omega_a t:t\in T_s\}$ is an orbit of the group $T_s$. This proves the statement (i) for $n=1$. In view of formulas (2.1), (2.7), and (4.2), this also implies the statement (i) for arbitrary $n$.

(ii) The above description of the structure of boxes $\Pi_a$ implies the following formula

$$\#\{\Pi_a\}=\begin{cases}1 & \text{if } \ a=0,\\ (q-1)q^{a-1} & \text{if } \ 1\leq a\leq s.\end{cases} \tag{4.6}$$

From (4.2), we conclude that

$$\#\{\Pi_A\}=\prod_{j=1}^{n}\#\{\Pi_{a_j}\}. \tag{4.7}$$

Substituting (4.6) into (4.7), we obtain (4.4).

(iii) Each orbit $\Pi_a$, $A\in Q_s^n$, can be identified with a homogeneous space: $\Pi_A\cong T_s^n/S(\Omega_A)$. Therefore,

$$\#\{\Pi_a\}=\frac{\#\{T_s^n\}}{\#\{S(\Omega_a)\}}\quad\text{or}\quad\#\{S(\Omega_A)\}=\frac{\#\{T_s^n\}}{\#\{\Pi_A\}}, \tag{4.8}$$

and formula (4.5) follows from (4.8), (4.4), and (2.9).

The proof of Lemma 4.1 is complete. □

Let two points $\Omega_1$ and $\Omega_2\in\mathrm{Mat}_{n,s}(\mathbb{F}_q)$ be given. What is the numbet of solutions $\tau\in T_s^n$ of the equation $\Omega_1\tau=\Omega_2$? We put

$$\mathcal{N}(\Omega_1,\Omega_2)=\{\tau\in T_s^n:\Omega_1\tau=\Omega_2\}\subset T_s^n \tag{4.9}$$

and

$$\nu(\Omega_1,\Omega_2)=\#\{\mathcal{N}(\Omega_1,\Omega_2)\}. \tag{4.10}$$

**Lemma 4.2.** (i) *If* $\Omega_1\in\Pi_{A_1}$, $\Omega_2\in\Pi_{A_2}$, *and* $A_1\neq A_2$, *then* $\nu(\Omega_1,\Omega_2)=0$.

(ii) *If* $\Omega_1\in\Pi_A$ *and* $\Omega_2\in\Pi_A$, *then* $\nu(\Omega_1,\Omega_2)=\#\{S(\Omega_A)\}$.

*Proof.* (i) The statement is a trivial consequence of Lemma 4.1(i).

(ii) Since both points $\Omega_1$ and $\Omega_2$ belong to the same orbit $\Pi_A$, we can write $\Omega_1=\Omega_A\tau_1$, $\Omega_2=\Omega_A\tau_2$ for a fixed point $\Omega_A\in\Pi_A$ and some $\tau_1$, $\tau_2\in T_s^n$. Therefore, the equation $\Omega_1\tau=\Omega_2$ takes the form $\Omega_A\tau_1\tau=\Omega_A\tau_2$ or $\Omega_A\tau_1\tau\tau_2^{-1}=\Omega_A$. This gives

$$\nu(\Omega_1,\Omega_2)=\#\{\tau\in T_s^n:\tau_1\tau\tau_2^{-1}\in S(\Omega_A)\}=\#\{\tau_1^{-1}S(\Omega_a)\tau_2\}=\#\{S(\Omega_A)\}.$$

The proof of Lemma 4.2 is complete. □

Now our interest is with the distribution of points of a code $\mathcal{C}\subset\mathrm{Mat}_{n,s}(\mathbb{F}_q)$ in boxes $\Pi_A$, $A\in Q_s^n$.

**Lemma 4.3.** *Let $\mathcal{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ be an arbitrary linear code. Then*

$$\#\{\mathcal{C} \cap \Pi_0\} = 1, \quad \#\{\mathcal{C} \cap \Pi_A\} = 0$$

*for $0 < a_1 + \cdots + a_n < \rho(\mathcal{C})$, and*

$$\#\{\mathcal{C} \cap \Pi_A\} \le q^{a_1 + \cdots + a_n - \rho(\mathcal{C}) + 1}$$

*for $a_1 + \cdots + a_n \ge \rho(\mathcal{C})$.*

This is Lemma 2.2 of [9].

Relying on the above three lemmas, we can easily complete the proof of Theorem 3.1.

## 5. Proof of Theorem 3.1

Let a linear code $\mathcal{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ be given. Fix a Hamming ball $B(d-1) \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ of radius $d-1$, where $d \ge 1$ is an integer (see (2.10)).

Let us split the group $T^n_s$ into a disjoint union of two subsets

$$T^n_s = \mathcal{G}(\mathcal{C}) \cup \mathcal{B}(\mathcal{C}),$$

where the subset $\mathcal{G}(\mathcal{C})$ of *"good"* transformations consists of all $\tau \in T^n_s$ such that $\Omega_1\tau \ne \Omega_2$ for all $\Omega_1 \in \mathcal{C} \setminus \{0\}$ and $\Omega_2 \in B(d-1) \setminus \{0\}$, and the subset $\mathcal{B}(\mathcal{C})$ of *"bad"* transformations consists of all $\tau \in T^n_s$ such that $\Omega_1\tau = \Omega_2$ at least for one pair $\Omega_1 \in \mathcal{C} \setminus \{0\}$ and $\Omega_2 \in B(d-1) \setminus \{0\}$.

From these definitions we immediately conclude that

$$\#\{\mathcal{G}(\mathcal{C})\} + \#\{\mathcal{B}(\mathcal{C})\} = \#\{T^n_s\}, \tag{5.1}$$

and

$$\varkappa(\mathcal{C}\tau) \ge d \tag{5.2}$$

for all transformations $\tau \in \mathcal{G}(\mathcal{C})$.

Let us estimate the cardinality of the subset of bad transformations. With definitions (4.9) and (4.10), we have

$$\mathcal{B}(\mathcal{C}) \subset \bigcup_{\Omega_1,\Omega_2} \{\mathcal{N}(\Omega_1,\Omega_2) : \Omega_1 \in \mathcal{C} \setminus \{0\}, \Omega_2 \in B(d-1) \setminus \{0\}\}$$

and

$$\mathcal{B}(\mathcal{C}) \le \sum_{\Omega_1,\Omega_2} \{\nu(\Omega_1,\Omega_2) : \Omega_1 \in \mathcal{C} \setminus \{0\}, \Omega_2 \in B(d-1) \setminus \{0\}\}\,. \tag{5.3}$$

Here, for simplicity, we write $\bigcup_{\alpha}\{\mathcal{E}_\alpha : \alpha \in \mathcal{O}\}$ instead of $\bigcup_{\alpha\in\mathcal{O}} \mathcal{E}_\alpha$ and $\sum_{\alpha}\{f(\alpha) : \alpha \in \mathcal{O}\}$ instead of $\sum_{\alpha\in\mathcal{O}} f(\alpha)$ if the corresponding region $\mathcal{O}$ is rather combersome to be indicated under the symbol of union or summation.

For short, we denote by $\Sigma_d(\mathcal{C})$ the sum in (5.3).

Using formula (4.3), we can write this sum in the form

$$\Sigma_d(\mathcal{C}) = \sum_{A_1,A_2\in Q_s^n} \sum_{\Omega_1,\Omega_2} \{\nu(\Omega_1,\Omega_2) : \Omega_1 \in \mathcal{C}\setminus\{0\}\cap\Pi_{A_1}, \Omega_2 \in B(d-1)\setminus\{0\}\cap\Pi_{A_2}\}\,. \tag{5.4}$$

By Lemma 4.2 (i), all terms in (5.4) with $A_1 \neq A_2$ vanish. Therefore,

$$\Sigma_d(\mathcal{C}) = \sum_{A\in Q_s^n} \sum_{\Omega_1,\Omega_2} \{\nu(\Omega_1,\Omega_2) : \Omega_1 \in \mathcal{C}\setminus\{0\}\cap\Pi_A, \Omega_2 \in B(d-1)\setminus\{0\}\cap\Pi_A\}$$

$$= \sum_{A\in Q_s^n\setminus\{0\}} \sum_{\Omega_1,\Omega_2} \{\nu(\Omega_1,\Omega_2) : \Omega_1 \in \mathcal{C}\cap\Pi_A, \Omega_2 \in B(d-1)\cap\Pi_A\}\,.$$

By Lemma 4.2 (ii) and Lemma 4.1 (iii), this equality can be continued as follows

$$\Sigma_d(\mathcal{C}) = \sum_{A\in Q_s^n\setminus\{0\}} \sum_{\Omega_1,\Omega_2} \{\#\{S(\Omega_A)\} : \Omega_1 \in \mathcal{C}\cap\Pi_A, \Omega_2 \in B(d-1)\cap\Pi_A\}$$

$$= \sum_{A\in Q_s^n\setminus\{0\}} \#\{S(\Omega_A)\}\#\{\mathcal{C}\cap\Pi_A\}\#\{B(d-1)\cap\Pi_A\}$$

$$= \#\{T_s^n\} \sum_{A\in Q_s^n\setminus\{0\}} \frac{\#\{\mathcal{C}\cap\Pi_A\}}{\#\{\Pi_a\}}\#\{B(d-1)\cap\Pi_A\}. \tag{5.5}$$

With Lemma 4.3 we obtain the following upper bound for the latest sum in (5.5)

$$\Sigma_d(\mathcal{C}) \leq \#\{T_s^n\}\sum_A \left\{\frac{q^{a_1+\cdots+a_n-\rho(\mathcal{C})+1}}{(q-1)^{\varkappa(A)}q^{a_1+\cdots+a_n-\varkappa(A)}}\#\{B(d-1)\cap\Pi_A\} : \right.$$
$$\left. A=(a_1,\dots,a_n)\in Q_s^n,\quad a_1+\cdots+a_n\geq\rho(\mathcal{C})\right\}$$

$$= \#\{T_s^n\}q^{-\rho(\mathcal{C})}\sum_A \left\{q\Big(\frac{q}{q-1}\Big)^{\varkappa(A)}\#\{B(d-1)\cap\Pi_A\} : \right.$$
$$\left. A=(a_1,\dots,a_n)\in Q_s^n,\quad a_1+\cdots+a_n\geq\rho(\mathcal{C})\right\}$$

$$\leq \#\{T_s^n\}q^{-\rho(\mathcal{C})}q\Big(\frac{q}{q-1}\Big)^n\sum_A \Big\{\#\{B(d-1)\cap\Pi_A\} : A=(a_1,\dots,a_n)\in Q_s^n,$$
$$\left. a_1+\cdots+a_n\geq\rho(\mathcal{C})\right\}$$

$$< \#\{T_s^n\}q^{-\rho(\mathcal{C})}q\Big(\frac{q}{q-1}\Big)^n\sum_{A\in Q_s^n}\{\#\{B(d-1)\cap\Pi_A\} = \#\{T_s^n\}q^{-\rho(\mathcal{C})}q\Big(\frac{q}{q-1}\Big)^n V_q(d-1), \tag{5.6}$$

where $V_q(d-1)$ is the volume of the ball $B(d-1)$ (see (2.11)).

Combining (5.3) and (5.6), we find the following upper bound for the cardinality of the subset of bad transformations

$$\#\{\mathcal{B}(\mathcal{C})\} < \#\{T_s^n\} q\Big(\frac{q}{q-1}\Big)^n V_q(d-1) q^{-\rho(\mathcal{C})}.$$

Substituting this inequality into (5.1), we find the following lower bound for the cardinality of the subset of good transformations

$$\frac{\#\{\mathcal{G}(\mathcal{C})\}}{\#\{T_s^n\}} > 1 - q\Big(\frac{q}{q-1}\Big)^n V_q(d-1) q^{-\rho(\mathcal{C})}. \tag{5.7}$$

Suppose that inequality (3.3) of Theorem 3.1 holds. Then, by (5.7) $\#\{\mathcal{G}(\mathcal{C})\} > 0$, and the subset $\mathcal{G}(\mathcal{C})$ is nonempty. Therefore, the bound (5.2) holds for all transformations $\tau \in \mathcal{G}(\mathcal{C})$.

The proof of Theorem 3.1 is complete. $\square$

**Acknowledgment.** The author is grateful to Michael Tsfasman and Serge Vladuţ for our many interesting and valuable discussions.

## References

1. W. W. L. Chen, M. M. Skriganov, *Explicit constructions in the classical mean squares problem in irregularities of point distribution*, J. reine angew. Math., **545** (2002), 67–95.
2. S. T. Dougherty, M. M. Skriganov, *MacWilliams duality and the Rosenbloom–Tsfasman metric*, Moscow Math. J., **2** (1) (2002), 81–97.
3. K. Lee, *Automorphism group of the Rosenbloom–Tsfasman space*, Eur. J. Combin., **24** (2003), 607–612.
4. J. H. van Lint, *Introduction to coding theory*, 3d ed., Graduate Texts Math., vol. 86, Springer-Verlag, Berlin (1999).
5. H. Niederreiter, C. P. Xing *Low-discrepancy sequences and global functional field with many rational point*, Finite Fields Appl., **2** (1996), 241–273.
6. E. Novak, H. Woźniakowski, *When are integration and discrepancy tactable?* in: FOCM Proceedings of Oxford (R. A. DeVore *et. al.* eds.) (1999), pp. 211–266, Cambridge Univ. Press (2001).
7. M. Yu. Rosenbloom, M. A. Tsfasman, *Codes for the m-metric*, Problemy Peredachi Informatsii, **33** (1) (1997), 55–63; English transl, in Problems Inform. Transmission **33** (1) (1997), 45–52.
8. M. M. Skriganov, *Coding theory and uniform distributions*, Algebra i Analiz **13** (2) (2001), 191–239; English transl. in St. Petersburg Math. J., **13** (2) (2002), 301–337.
9. M. M. Skriganov, *Harmonic analysis on totally disconnected groups and irregularities of point distributions*, J. reine angew. Math. (to appear).