On q-analog Steiner systems of rank metric codes

Francisco Arias[1], Javier de la Cruz[1,2*], Joachim Rosenthal[2†] and Wolfgang Willems[1,3]

[1]Universidad del Norte, Barranquilla, Colombia
[2]University of Zurich, Switzerland
[3]Otto-von-Guericke Universität, Magdeburg, Germany

September 25, 2017

Abstract

In this paper we prove that rank metric codes with special properties imply the existence of q-analogs of suitable designs. More precisely, we show that the minimum weight vectors of a $[2d, d, d]$ dually almost MRD code $C \leq \mathbb{F}_{q^m}^n$ which has no code words of rank weight $d+1$ form a q-analog Steiner system $S_q(d-1, d, 2d)$. In particular, $d+1$ must be a prime.

Keywords: Rank metric code, q-analog Steiner system, dually AMRD code

Mathematics Subject Classification: 94B05, 94B60, 05B25, 51E10

1 Introduction

The interest in q-analogs of codes and designs has been increased over the last years due to their applications in random network coding. One of the most challenging problems is the existence of q-analogs of Steiner systems, in particular of the Fano plane.

The paper is structured as follows. In Section 2 we collect some facts on rank metric codes, in particular on generalized rank weights. Section 3 deals with Gaussian binomial coefficients and cyclotomic polynomials. In Section 4 we analyze the supports of the minimum weight vectors of a rank metric code. Section 5 deals with a relationship between rank metric codes and q-analog designs. We prove that the minimum weight vectors of a $[2d, d, d]$ dually almost MRD code $C \leq \mathbb{F}_{q^m}^n$ which has no code words of rank weight $d+1$ hold a $S_q(d-1, d, 2d)$ Steiner system. In particular $d+1$ must be a prime. Note that apart from trivial examples only $S_2(2, 3, 13)$ is known to exist [2].

*This work was done while J. de la Cruz was at the University of Zurich supported by the Swiss Confederation through the Swiss Government Excellence Scholarship no. 2016.0873. The autor was partially supported by COLCIENCIAS through project no. 121571250178.

†J. Rosenthal was supported in part by the Swiss National Science Foundation under grant no. 169510.

2 Preliminaries

In this paper we study $\mathbb{F}_{q^m}$-linear codes $C \leq \mathbb{F}_{q^m}^n$ endowed with the rank metric distance. To be more precise, note that the field $\mathbb{F}_{q^m}$ may be viewed as an m-dimensional vector space over $\mathbb{F}_q$. The *rank weight*, or briefly the *weight* of a vector $v = (v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$ is defined as the maximum number of coordinates in v that are linearly independent over $\mathbb{F}_q$, i.e., $\mathrm{wt}(v) = \dim_{\mathbb{F}_q} \langle v_1, \ldots, v_n \rangle$. For $v, u \in \mathbb{F}_{q^m}^n$ the rank metric distance is then given by $\mathrm{d}(v, u) = \mathrm{wt}(u - v) = \mathrm{rank}(v - u)$.

An $\mathbb{F}_{q^m}$-linear subspace $C \leq \mathbb{F}_{q^m}^n$ of dimension k endowed with this metric is called an $[n, k]$ $\mathbb{F}_{q^m}$*-linear rank metric* code. As usual the minimum distance of $C \neq \{0\}$ is defined by

$$\mathrm{d} = \mathrm{d}(C) = \min\{\mathrm{wt}(c) \mid 0 \neq c \in C\}.$$

By $A_i(C)$ we always denote the code words of C of weight i. Finally, we use the notation $C^\perp$ for the orthogonal of C which is taken with respect to the standard inner product of $\mathbb{F}_{q^m}^n$.

Throughout the paper we always assume that $C \leq \mathbb{F}_{q^m}^n$ is an $\mathbb{F}_{q^m}$-linear rank metric code with minimum distance d. Furthermore we assume that C is not trivial, i.e., $0 \neq C \neq \mathbb{F}_{q^m}^n$ and $n \leq m$. Thus, if $\dim C = k$, then the last condition implies the Singleton bound

$$d \leq n - k + 1.$$

C is called a *maximum rank distance code*, shortly an MRD code, if the bound is achieved. Delsarte [8] and independently Gabidulin [11] proved the existence of such codes for all q, m, n and dimension $1 \leq k \leq n$ (here $n \leq m$ is not necessary). Given the parameters q, m, n, k, the code $C \leq \mathbb{F}_{q^m}^n$ these authors describe has a particular construction through a generator matrix $M_k(v)$ and the resulting code is usually called a Gabidulin code. Recently other new constructions of MRD codes have been found which are not equivalent to Gabidulin codes ([6, 18]). Somehow surprisingly, over the algebraic closure, the set of MRD codes forms a generic set inside the Grassmann variety of all k-dimensional linear subspaces of $\mathbb{F}_{q^m}^n$ [16]. In particular over some large finite field there exist large numbers of MRD codes and lower bounds on these cardinalities can be found in [16].

In analogy to the Singleton defect for classical codes as given in [7, 10], we have the following definition for the defect of rank metric codes [5].

Definition 2.1. The *rank defect*, briefly the *defect*, of an $\mathbb{F}_{q^m}$-linear $[n, k, d]$ rank metric code $C \leq \mathbb{F}_{q^m}^n$ is defined by $\mathrm{def}(C) = n - k + 1 - d$.

Note that $\mathrm{def}(C) = 0$ if and only if C is an MRD code. Other interesting codes which are coming close to MRD codes, are the so-called *dually almost* MRD codes or simply *dually* AMRD codes [4]. More precisely, we say that a $\mathbb{F}_{q^m}$-linear rank metric code C is dually AMRD if $\mathrm{def}(C) = \mathrm{def}(C^\perp) = 1$. Dually AMRD codes are subject of the main results in the last section of this paper. These codes can be viewed as a q-analogon of a

classical almost-MDS (AMDS) code and as in the classical situation these codes induce again some q-Steiner system.

Let $b_1, \ldots, b_m$ be a basis B of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. For $v = (v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$ we write

$$v_i = \sum_{j=1}^{m} \alpha_{ji} b_j$$

and put $M_B(v) = (\alpha_{ji}) \in (\mathbb{F}_q)^{m \times n}$. As mentioned in ([13], Section 2), the K-linear row space of $M_B(v)$ is independent of the chosen basis B.

In order to define generalized rank weights we need the following notations [12, 13].

Definition 2.2. For $v = (v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$ and an $\mathbb{F}_{q^m}$-linear subspace V of $\mathbb{F}_{q^m}^n$ we define

a) $\mathrm{supp}(v)$ as the $\mathbb{F}_q$-linear row space of $M_B(v)$.

b) $\mathrm{supp}(V) = \langle \mathrm{supp}(v) \mid v \in V \rangle$ as an $\mathbb{F}_q$-vector space.

c) $\mathrm{wt}(V) = \dim \mathrm{supp}(V)$.

d) $V^\star = \sum_{i=0}^{m-1} V^{q^i}$.

In the literature there are different definitions for generalized rank weights (see [17],[15], [9], [13]). All of them define the same numbers. For our purpose the definition given in [13] seems to be the most appropriate.

Definition 2.3. The *r-th generalized rank weight* d_r of a rank metric code $C \leq \mathbb{F}_{q^m}^n$ is defined by

$$\mathrm{d}_r(C) = \min_{\substack{D \leq C \\ \dim D = r}} \mathrm{wt}(D).$$

Combining results of [15],[9] and [13] we obtain the rank metric analog of Wei's result [19] on generalized Hamming weights.

Theorem 2.4. *If C is an $\mathbb{F}_{q^m}$-linear rank metric code in $\mathbb{F}_{q^m}^n$ of dimension k and minimum distance d, then*

$$\mathrm{d}(C) = \mathrm{d}_1(C) < \mathrm{d}_2(C) < \ldots < \mathrm{d}_k(C).$$

Proof. We have

$$\begin{aligned}
\mathrm{d}_r(C) &= \min_{\substack{D \leq C \\ \dim D = r}} \mathrm{wt}(D) \\
&= \min_{\substack{D \leq C \\ \dim D = r}} \dim D^\star && ([13], \text{Corollary 4.4}) \\
&= \min_{\substack{D \leq C \\ \dim D = r}} \max_{d \in D^\star} \mathrm{wt}(d) && ([13], \text{Theorem 5.8}) \\
&= \min_{\substack{V = V^\star \\ \dim(C \cap V) \geq r}} \dim V && ([9], \text{Proposition II.1}) \\
&= \mathcal{M}_r(C). && (\text{Definition 5 in } [15])
\end{aligned}$$

By ([15], Lemma 9) we get

$$\mathcal{M}_1(C) < \ldots < \mathcal{M}_k(C),$$

and the proof is complete since obviously $\mathrm{d}(C) = \mathrm{d}_1(C)$. $\square$

3 Gaussian binomial coefficients and cyclotomic polynomials

The results of this section are known but crucial for the rest of the paper. Since they are hard to find in the literature we will state them with proofs for the reader's convenience.

Definition 3.1. Let q be a prime power and let a and b be non-negative integers. The q-ary Gaussian binomial coefficient of a over b is defined by

$$\begin{bmatrix} a \\ b \end{bmatrix}_q = \begin{cases} \frac{(q^a-1)(q^{a-1}-1)\ldots(q^{a-b+1}-1)}{(q^b-1)(q^{b-1}-1)\ldots(q-1)} & \text{if } b \leq a \\ 0 & \text{if } b > a \end{cases}$$

Throughout the paper we freely use the symmetry of the Gaussian binomial coefficients; i.e., $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]_q = \left[\begin{smallmatrix} a \\ a-b \end{smallmatrix}\right]_q$ for $b \leq a$.

Furthermore $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]_q$ can be expressed by suitable $\Phi_n(q)$ where $\Phi_n(x)$ denotes the n-th cyclotomic polynomial defined by

$$\Phi_n(x) = \prod_{\substack{1 \leq i \leq n \\ \gcd(j,n)=1}} (x - \zeta_n^j)$$

where ζ_n is a primitive complex n-th root of unity. Recall that $\Phi_n(x)$ is an irreducible polynomial in $\mathbb{Z}[x]$. For $n \in \mathbb{N}$ we put $[n] = \{1, 2, \ldots, n\}$.

Proposition 3.2. *For $b < a$ we have*

$$\begin{bmatrix} a \\ b \end{bmatrix}_q = \prod_{j \in J_{a,b}} \Phi_j(q)$$

where $J_{a,b} = \{j \in [a] \mid ((a-b) \bmod j) + (b \bmod j) \geq j\}$.

Proof. By ([3], Lemma 1), we have

$$\begin{bmatrix} a \\ b \end{bmatrix}_q = \prod_{j=1}^{a} \Phi_j(q)^{\lfloor \frac{a}{j} \rfloor - \lfloor \frac{b}{j} \rfloor - \lfloor \frac{a-b}{j} \rfloor}.$$

Furthermore, since

$$0 \leq \lfloor \frac{a}{j} \rfloor - \lfloor \frac{b}{j} \rfloor - \lfloor \frac{a-b}{j} \rfloor \leq 1$$

we obtain

$$\begin{bmatrix} a \\ b \end{bmatrix}_q = \prod_{j \in J} \Phi_j(q)$$

where $J = \{j \in [a] \mid \lfloor \frac{a}{j} \rfloor = \lfloor \frac{b}{j} \rfloor + \lfloor \frac{a-b}{j} \rfloor + 1\}$. Thus we need to show that $J = J_{a,b}$. If we write $a = \lfloor \frac{a}{j} \rfloor j + r_a$ with $0 \leq r_a < j$ and similarly b and $a - b$ we get

$$a = \left(\left\lfloor \frac{b}{j} \right\rfloor + \left\lfloor \frac{a-b}{j} \right\rfloor \right) j + r_b + r_{a-b}.$$

Thus $j \in J$ if and only if

$$r_b + r_{a-b} - j = r_a \geq 0$$

if and only if

$$r_b + r_{a-b} \geq j.$$

The last condition says nothing else than

$$(b \bmod j) + ((a-b) \bmod j) \geq j.$$

□

Lemma 3.3. *Let $a, d \in \mathbb{N}$. If p is a prime with $p \mid d+1$ and $p \mid c$, then $c \notin J_{d+p,p-1}$.*

Proof. Write $d + 1 = xc + r$ with $x \in \mathbb{N}$ and $0 \leq r < c$. Since $p \mid d+1$ and $p \mid c$ we have $p \mid r$. Suppose that $c \in J_{d+p,p-1}$. Thus

$$((d+1) \bmod c) + ((p-1) \bmod c) \geq c.$$

This implies that $r + (p-1) \geq c$, hence $c > r \geq c - p + 1$. Thus we obtain $r = c - p + i$ where $i \in \{1, \ldots, p-1$, which is a contradiction since $p \mid r$ and $p \mid c$. □

Lemma 3.4. *Let p be a prime and $c \in \mathbb{N}$. If $\gcd(\Phi_p(q), \Phi_c(q)) > 1$, then $p \mid c$.*

Proof. The assumption $\gcd(\Phi_p(q), \Phi_c(q)) > 1$ implies that $\gcd(q^p - 1, q^c - 1) > 1$. From finite field theory we know that

$$\gcd(q^p - 1, q^c - 1) = q^{\gcd(p,c)} - 1.$$

Thus, if $p \nmid c$, then $\gcd(q^p - 1, q^c - 1) = q - 1 = \Phi_1(q)$. Since

$$q^p - 1 = \Phi_1(q)\Phi_p(q)$$

and

$$q^c - 1 = \Phi_1(q) \prod_{1 \neq t \mid c} \Phi_t$$

we obtain $\gcd(\Phi_p(q), \Phi_c(q)) = 1$, a contradiction. □

4 Supports of the minimum weight vectors

From paper [13] we know the following facts.

Lemma 4.1. *Let $C \leq \mathbb{F}_{q^m}^n$ be an $\mathbb{F}_{q^m}$-linear rank metric code.*

a) *If $u = \alpha v$ for some $\alpha \in \mathbb{F}_{q^m}$, then* $\mathrm{supp}(v) = \mathrm{supp}(u)$.

b *If $v_1, \ldots, v_k \in \mathbb{F}_{q^m}^n$ generate C, then*

$$\mathrm{supp}(C) = \sum_{i=1}^{k} \mathrm{supp}(v_i).$$

c) *There exists an element $c \in C$ such that*

$$\mathrm{supp}(c) = \mathrm{supp}(C).$$

d) *For $u, v \in \mathbb{F}_{q^m}^n$ there exist $\alpha, \beta \in \mathbb{F}_{q^m}$ such that* $\mathrm{supp}(\alpha v + \beta u) = \mathrm{supp}(v) + \mathrm{supp}(u)$.

Proof. a) and b) are part of Proposition 2.3 of [13]. c) is Proposition 3.6 and d) Proposition 3.9 of the same paper. □

Definition 4.2. For an $\mathbb{F}_{q^m}$-linear rank metric code $C \leq \mathbb{F}_{q^m}^n$ of dimension k and minimum distance d we put

$$D_i(C) = \{\mathrm{supp}(c) \mid c \in C,\ \mathrm{wt}(c) = i\}$$

for $i = 0, d, \ldots, n - k + 1$.

Lemma 4.3. *Let $C \leq \mathbb{F}_{q^m}^n$ be an $\mathbb{F}_{q^m}$-linear rank metric code with minimum distance d.*

a) *Let $v, u \in C$ and* $\mathrm{wt}(v) = \mathrm{wt}(u) = d$. *Then* $\mathrm{supp}(v) = \mathrm{supp}(u)$ *if and only if there exists $\alpha \in \mathbb{F}_{q^m}^\star$ such that $u = \alpha v$.*

b) $|D_d(C)| = \frac{A_d(C)}{q^m - 1}$.

Proof. a) One direction follows by Lemma 4.1 a). Suppose $\mathrm{supp}(v) = \mathrm{supp}(u)$ and v, u linearly independent over $\mathbb{F}_{q^m}$. Let $W = \langle v, u \rangle$ as a vector space over $\mathbb{F}_{q^m}$. By Lemma 4.1 b), we get $\mathrm{supp}(W) = \mathrm{supp}(v) + \mathrm{supp}(u) = \mathrm{supp}(v)$. Therefore

$$\mathrm{wt}(W) = \dim_{\mathbb{F}_q}(\mathrm{supp}(W)) = \dim_{\mathbb{F}_q}(\mathrm{supp}(v)) = d.$$

Thus, according to the definition of generalized rank weights we obtain

$$d_2(C) = \min\{\mathrm{wt}_R(S) \mid S \leq C \text{ and } \dim_{\mathbb{F}_{q^m}} S = 2\} = d,$$

which contradicts Theorem 2.4.
b) This immediately follows from part a). □

5 q-analog Steiner systems and rank metric codes

Maximum distance separable (MDS) codes are $[n, k, d]$ linear codes $C \leq \mathbb{F}_q^n$ which reach the Singleton bound $d = n - k + 1$. Almost-MDS (AMDS) codes were introduced by de Boer [7] and they are characterized that their Singleton defect is one, i.e. $d = n - k$.

In [10] it has been shown that the supporters of code words of minimum weight of a $[2d, d, d]$ dually AMDS code ($d \geq 2$) which has no code words of weight $d + 1$ form the blocks of an $S(d-1, d, 2d)$ classical Steiner system and $d+1$ must be a prime. For instance, in this way the extended ternary Golay code leads to an $S(5, 6, 12)$ Steiner system. In this section we prove the q-analog of this result.

Definition 5.1. Let $t \leq k \leq n$ be natural numbers. A q-Steiner system $S_q(t, k, n)$ is a set of k-dimensional subspaces of $\mathbb{F}_q^n$, called the blocks, such that every t-dimensional subspace of $\mathbb{F}_q^n$ is contained in exactly one block.

Note that the number of blocks of an $S_q(t, k, n)$ Steiner system is $\frac{\begin{bmatrix} n \\ t \end{bmatrix}_q}{\begin{bmatrix} k \\ t \end{bmatrix}_q}$.

Lemma 5.2. *A $S_q(t, k, n)$ Steiner system implies an $S_q(t-1, k-1, n-1)$ Steiner system if $t \geq 2$.*

Proof. This is one part of ([14], Lemma 5). □

Theorem 5.3. *Let $C \leq \mathbb{F}_{q^m}^{2d}$ be a $[2d, d, d]$ dually AMRD code with $d \geq 2$ and $A_{d+1}(C) = 0$. Then the set $D_d(C)$ are the blocks of an $S_q(d-1, d, 2d)$ Steiner system.*

Proof. (i) Let $W \leq \mathbb{F}_q^{2d}$ be of dimension $d-1$. Suppose that W is contained in two different blocks, i.e., elements of $D_d(C)$. Hence

$$W \subseteq \operatorname{supp}(u) \cap \operatorname{supp}(v)$$

with $\operatorname{supp}(u), \operatorname{supp}(v) \in D_d(C)$. Since $\dim(\operatorname{supp}(u) \cap \operatorname{supp}(v)) \leq d - 1$ we obtain

$$W = \operatorname{supp}(u) \cap \operatorname{supp}(v).$$

Thus

$$\dim(\operatorname{supp}(u) + \operatorname{supp}(v)) = 2d - (d - 1) = d + 1.$$

By Lemma 4.1 d) there are $\alpha, \beta \in \mathbb{F}_{q^m}$ such that

$$\operatorname{supp}(u) + \operatorname{supp}(v) = \operatorname{supp}(\alpha u + \beta v).$$

Thus $\alpha u + \beta v \in C$ has weight $d + 1$, a contradiction. This means that every $(d - 1)$-dimensional subspace of $\mathbb{F}_q^{2d}$ is contained in at most one block.

(ii) According to Lemma 4.3 b) we have $|D_d(C)| = \frac{A_d(C)}{q^m - 1}$. Since $A_{d+1}(C) = 0$, Theorem 25 of [5] yields

$$A_d(C) = \frac{\begin{bmatrix} 2d \\ d+1 \end{bmatrix}_q}{\begin{bmatrix} d \\ 1 \end{bmatrix}_q}(q^m - 1) = \frac{\begin{bmatrix} 2d \\ d-1 \end{bmatrix}_q}{\begin{bmatrix} d \\ d-1 \end{bmatrix}_q}(q^m - 1),$$

hence $|D_d(C)| = \frac{\begin{bmatrix} 2d \\ d-1 \end{bmatrix}_q}{\begin{bmatrix} d \\ d-1 \end{bmatrix}_q}$. Since each block contains exactly $\begin{bmatrix} d \\ d-1 \end{bmatrix}_q$ subspaces of dimension $(d-1)$ and every $(d-1)$-dimensional subspace is contained in at most one block by (i), the blocks altogether contain

$$|D_d(C)| \begin{bmatrix} d \\ d-1 \end{bmatrix}_q = \begin{bmatrix} 2d \\ d-1 \end{bmatrix}_q$$

subspaces of dimension $d-1$. As $\begin{bmatrix} 2d \\ d-1 \end{bmatrix}_q$ is the number of $(d-1)$-dimensional subspaces in a space of dimension $2d$, the proof is complete. □

Remark 5.4. Let $C \leq \mathbb{F}_{q^m}^{2d}$ be a $[2d, d, d]$ dually AMRD code with $d \geq 2$ and $A_{d+1}(C) = 0$. Then $C^\perp$ also leads to an $S_q(d-1, d, 2d)$ Steiner system, since C is formally self-dual, by ([4], Lemma 4.11).

Example 5.5. Let C be the $\mathbb{F}_{2^4}$-linear $[4, 2, 2]$ code with generator matrix

$$\begin{pmatrix} 0 & 1 & \omega & 0 \\ 1 & 0 & 0 & \omega \end{pmatrix}$$

where ω is a primitive third root of unity in $\mathbb{F}_{2^4}^\star$. With Magma [1] we get $A_0(C) = A_0(C^\perp) = 1$, $A_2(C) = A_2(C^\perp) = 75$, $A_3(C) = A_3(C^\perp) = 0$ and $A_4(C) = A_4(C^\perp) = 180$. Thus C is a $[4, 2, 2]$ dually almost MRD code over $\mathbb{F}_{2^4}$. Consequently, by Theorem 5.3 the elements of $D_d(C)$ are the blocks of an $S_2(4, 2, 1)$ Steiner system. Note that this 2-Steiner system is one of the trivial ones.

Remarks 5.6. a) According to Theorem 5.3 a $[8, 4, 4]$ dually AMRD code over $\mathbb{F}_{2^8}$ with $A_5(C) = 0$ implies the existence of a Steiner system $S_2(3, 4, 8)$. Thus, by Lemma 5.2, the existence of the code would imply the existence of an $S_2(2, 3, 7)$ Steiner system which is the 2-analog of the Fano plane.
b) By Theorem 5.3 and Lemma 5.2, a $[2d, d, d]$ dually AMRD code over $\mathbb{F}_{q^m}$ with $d \geq 2$ and $A_{d+1}(C) = 0$ implies an $S_q(1, 2, d+2)$ Steiner system. It follows that $q^2 - 1 \mid q^{d+2} - 1$. Thus d must be even.

Theorem 5.7. *Let $C \leq \mathbb{F}_{q^m}^{2d}$ be a $[2d, d, d]$ dually AMRD code with $d \geq 2$ and $A_{d+1}(C) = 0$. Then $d+1$ is a prime.*

Proof. Let p be a prime with $p \mid d+1 \neq p$, hence $d+1 = px$ with $x \geq 2$. By Theorem 5.3, there exists a Steiner system $S_q(d-1, d, 2d)$. Since $p-1 \leq d-1$ Lemma 5.2 implies the existence of an $S_q(p-1, p, d+p)$ Steiner system. This Steiner system has exactly

$$\frac{\begin{bmatrix} d+p \\ p-1 \end{bmatrix}_q}{\begin{bmatrix} p \\ p-1 \end{bmatrix}_q} = \frac{\begin{bmatrix} d+p \\ p-1 \end{bmatrix}_q}{\begin{bmatrix} p \\ 1 \end{bmatrix}_q} \in \mathbb{N}$$

blocks. According to Proposition 3.2 we obtain

$$\frac{\begin{bmatrix} d+p \\ p-1 \end{bmatrix}_q}{\begin{bmatrix} p \\ 1 \end{bmatrix}_q} = \frac{\prod_{j \in J_{d+p,p-1}} \Phi_j(q)}{\prod_{j \in J_{p,1}} \Phi_j(q)} = \frac{\prod_{j \in J_{d+p,p-1}} \Phi_j}{\Phi_p(q)} \in \mathbb{N}.$$

Thus exists a $c \in J_{d+p,p-1}$ such that $1 < \gcd(\Phi_p(q), \Phi_c(q))$. Lemma 3.4 implies that $p \mid c$ and according to Lemma 3.3 we get $c \notin J_{d+p,p-1}$, a contradiction. Thus $d+1 = p$ and we are done. $\square$

References

[1] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system I: The user language, *J. Symbolic Computation* **24** (1997), 235-265.

[2] M. Braun, T. Etzion, P.R.J. Östergård, A. Vardy and A. Wassermann, *Existence of q-analogs of Steiner systems*, Forum Math. Pi**4** (2016), e7, 14pp.

[3] W. Y.C. Chen, Q.-H. Hou, Factors of the Gaussian coefficients, *Discrete Mathematics* **306** (2006), 1446-1449.

[4] J. de la Cruz, On dually almost MRD codes, `https://arxiv.org/abs/1612.04268`.

[5] J. de la Cruz, E. Gorla, H. López, A. Ravagnani, Weight distribution of rank-metric codes, *Designs, Codes and Cryptography*, (2017), doi:10.1007/s10623-016-0325-1.

[6] J. de la Cruz, M. Kiermaier, A. Wassermann and W. Willems, Algebraic structures of MRD Codes, *Adv. Math. Commun.* **10** (2016), 499-510.

[7] M. A. de Boer. Almost MDS codes. *Des. Codes Cryptogr.*, 9(2):143–155, 1996.

[8] P. Delsarte, Bilinear forms over a finite field, with applications to coding theory, *J. Combin. Theory Ser.* A **25** (1978), 226-241.

[9] J. Ducoat, Generalized rank weights: duality and Griesmer bound, `http://arxiv.org/abs/1306.3899v1`

[10] A. Faldum and W. Willems, Codes of small defect, *Designs, Codes and Cryptography*, 10 (1997) 341-350.

[11] E. M. Gabidulin, Theory of codes with maximum rank distance, *Probl. Inf. Transm.*, Vol. **21** (1985) 1-12.

[12] A.-L. Horlemann-Trautmann, K. Marshall, J. Rosenthal, Extension of Overbeck's attack for Gabidulin-based cryptosystems, *Designs, Codes and Cryptography*, (2017), 1-22.

[13] R. Jurrius and R. Pellikann, On defining generalized rank weights, *Adv. Math. Commun.* **11** (2017), 225-235.

[14] M. Kiermaier and R. Laue, Derived and residual subspace designs, *Adv. Math. Commun.* **9** (2015), 105-110.

[15] J. Kurihara, R. Matsumoto, and T. Uyematsu, Relative generalized rank weight of linear codes and its applications to network coding, *Transactions on Information Theory* **61** (2015), 3912-3936.

[16] A. Neri, A.-L. Horlemann-Trautmann, T. Randrianarisoa, and J. Rosenthal. On the genericity of maximum rank distance and Gabidulin codes. *Designs, Codes and Cryptography*, 85, 2017. doi:10.1007/s10623-017-0354-4.

[17] F. Oggier and A. Sboui A, On the existence of generalized rank weights, *in Proc. 2012 Int. Symp. Information Theory and Its Applications, Honolulu, Hawaii, USA*, 406-410.

[18] J. Sheekey, A new family of linear maximum rank distance codes, *Adv. Math. Commun.* **10** (2016), 475-488.

[19] V. K. Wei, Generalized Hamming weights for linear codes, *IEEE Trans. Inf. Theory* **37** (1991), 1412-1418.