Subspace codes in PG(2n-1,q)

Subspace codes in PG$(2n-1, q)$

Antonio Cossidente
Dipartimento di Matematica, Informatica ed Economia
Università della Basilicata
Contrada Macchia Romana
I-85100 Potenza
Italy
antonio.cossidente@unibas.it
Francesco Pavese
Dipartimento di Matematica, Informatica ed Economia
Università della Basilicata
Contrada Macchia Romana
I-85100 Potenza
Italy
francesco.pavese@unibas.it

Proposed Running Head: Subspace codes in $\mathrm{PG}(2n-1, q)$

Corresponding Author:
Francesco Pavese
Dipartimento di Matematica, Informatica ed Economia
Università della Basilicata
Contrada Macchia Romana
I-85100 Potenza
Italy
francesco.pavese@unibas.it

Abstract

An $(r, M, 2\delta; k)_q$ constant–dimension subspace code, $\delta > 1$, is a collection $\mathcal{C}$ of $(k-1)$–dimensional projective subspaces of $\mathrm{PG}(r-1, q)$ such that every $(k-\delta)$–dimensional projective subspace of $\mathrm{PG}(r-1, q)$ is contained in at most a member of $\mathcal{C}$. Constant–dimension subspace codes gained recently lot of interest due to the work by Koetter and Kschischang [20], where they presented an application of such codes for error–correction in random network coding. Here a $(2n, M, 4; n)_q$ constant–dimension subspace code is constructed, for every $n \geq 4$. The size of our codes is considerably larger than all known constructions so far, whenever $n > 4$. When $n = 4$ a further improvement is provided by constructing an $(8, M, 4; 4)_q$ constant–dimension subspace code, with $M = q^{12} + q^2(q^2+1)^2(q^2+q+1) + 1$.

KEYWORDS: hyperbolic quadric; subspace code; Segre variety; rank distance codes.
AMS MSC: 51E20, 05B25, 94B27, 94B60, 94B65.

1 Introduction

Let V be an r–dimensional vector space over $\mathrm{GF}(q)$, q any prime power. The set $S(V)$ of all subspaces of V, or subspaces of the projective space $\mathrm{PG}(V)$, forms a metric space with respect to the *subspace distance* defined by $d_s(U, U') = \dim(U + U') - \dim(U \cap U')$. In the context of subspace coding theory, the main problem asks for the determination of the larger size of codes in the space $(S(V), d_s)$ (*subspace codes*) with given minimum distance and of course the classification of the corresponding optimal codes. Codes in the projective space and codes in the Grassmannian over a finite field referred to as subspace codes and constant–dimension codes (CDCs), respectively, have been proposed for error control in random linear network coding, see [20]. An $(r, M, d; k)_q$ constant–dimension subspace code is a set $\mathcal{C}$ of k–subspaces of V, where $|\mathcal{C}| = M$ and minimum subspace distance $d_s(\mathcal{C}) = \min\{d_s(U, U') \mid U, U' \in \mathcal{C}, U \neq U'\} = d$. The maximum size of an $(r, M, d; k)_q$ constant–dimension subspace code is denoted by $\mathcal{A}_q(r, d; k)$.

The upper bounds on $\mathcal{A}_q(r, d; k)$ are usually the q–analog of the bounds obtained for the well studied constant weight codes. In particular the following upper bound has been proved in [27] and [9].

$$\mathcal{A}_q(r, d; k) \leq \left\lfloor \frac{q^r - 1}{q^k - 1} \left\lfloor \frac{q^{r-1} - 1}{q^{k-1} - 1} \cdots \left\lfloor \frac{q^{r-k+d} - 1}{q^d - 1} \right\rfloor \cdots \right\rfloor \right\rfloor . \tag{1}$$

For general results on bounds and constructions of subspaces codes, see [17]. More recent constructions and results can be found in [7], [8], [9], [11], [15], [26]. For a geometric approach to subspace codes see also [3], where a connection between certain subspace codes and particular combinatorial structures is highlighted.

From a combinatorial point of view an $(r, M, 2\delta; k)_q$ constant–dimension subspace code, $\delta > 1$, is a collection $\mathcal{C}$ of $(k-1)$–dimensional projective subspaces of $\mathrm{PG}(r-1, q)$ such that every $(k-\delta)$–dimensional projective subspace of $\mathrm{PG}(r-1, q)$ is contained in at most a member of $\mathcal{C}$.

The set $\mathcal{M}_{m\times n}(q)$ of $m \times n$ matrices over the finite field $\mathrm{GF}(q)$ forms a metric space with respect to the *rank distance* defined by $d_r(A, B) = rk(A - B)$. The maximum size of a code of minimum distance d, $1 \leq d \leq \min\{m, n\}$, in $(\mathcal{M}_{m\times n}(q), d_r)$ is $q^{n(m-d+1)}$ for $m \leq n$ and $q^{m(n-d+1)}$ for $m \geq n$. A code $\mathcal{A} \subset \mathcal{M}_{m\times n}(q)$ attaining this bound is said to be a q–ary (m, n, k) *maximum rank distance code* (*MRD*), where $k = m - d + 1$ for $m \leq n$ and $k = n - d + 1$ for $m \geq n$. A rank code $\mathcal{A}$ is called $\mathrm{GF}(q)$–linear if $\mathcal{A}$ is a subspace of $\mathcal{M}_{m\times n}(q)$. Rank metric codes were introduced by Delsarte [5] and rediscovered in [10] and [23]. For the construction of non–linear maximum rank distance codes, see also [4].

Recently, these codes have found a new application in the construction of error–correcting codes for random network coding [25]. Indeed, as regard as lower bounds on $\mathcal{A}_q(r, d; k)$, in [25] there is a construction of CDC based on maximum rank distance codes, which yields the bound $\mathcal{A}_q(r, d; k) \geq q^{(r-k)(k-d+1)}$. Athough the size of the code $\mathcal{C}$ constructed from an MRD code equals the highest power of q in the upper bound (1), it is known that $\mathcal{C}$ is not maximal and that can be extended.

A *constant–rank code* (CRC) of constant rank r in $\mathcal{M}_{m\times n}(q)$ is a non–empty subset of $\mathcal{M}_{m\times n}(q)$ such that all elements have rank r. We denote a constant–rank code with length n, minimum rank distance d, and constant–rank r by (m, n, d, r). The term $A(m, n, d, r)$ denotes the maximum cardinality of an (m, n, d, r) constant–rank code in $\mathcal{M}_{m\times n}(q)$. From [11, Proposition 8] we have that $A(m, n, d, r) \leq \begin{bmatrix} n \\ r \end{bmatrix}_q \prod_{i=0}^{r-d} (q^m - q^i)$ and if this upper bound is attained the CRC is said to be optimal. Here $\begin{bmatrix} n \\ r \end{bmatrix}_q := \frac{(q^n-1)\cdot\ldots\cdot(q^{n-r+1}-1)}{(q^r-1)\cdot\ldots\cdot(q-1)}$.

In this paper we will construct a $(2n, M, 4; n)_q$ constant–dimension subspace code, for every $n \geq 4$. The size of our codes is considerably larger than all known constructions so far whenever $n > 4$ (Theorem 3.8, Theorem 3.11). Our approach is completely geometric and relies on the geometry of Segre varieties. This point of view enabled us to improve the construction of CDC arising from an MRD code by means of certain CRCs and the geometry of a non–degenerate hyperbolic quadric of the ambient projective space.

When $n = 4$, by exploring in more details the geometry of the hyperbolic quadric $\mathcal{Q}^+(7,q)$, a further improvement is provided by constructing an $(8, M, 4; 4)_q$ constant–dimension subspace code, with $M = q^{12} + q^2(q^2 + 1)^2(q^2+q+1)+1$. A $(8, M, 4; 4)_q$, with $M = q^{12}+q^2(q^2+1)^2(q^2+q+1)+1$ has also been constructed in [7] with a completely different technique. We do not know if the two constructions are equivalent but certainly both codes contain a lifted MRD code.

In the sequel $\theta_{n,q} := \begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q = q^n + \ldots + q + 1$.

2 The geometric setting

2.1 Segre variety and Veronese variety

The *Segre map* may be defined as the map

$$\sigma : \mathrm{PG}(n-1,q) \times \mathrm{PG}(m-1,q) \to \mathrm{PG}(nm-1,q),$$

taking a pair of points $x = (x_1, \ldots x_n)$ of $\mathrm{PG}(n-1,q)$, $y = (y_1, \ldots y_m)$ of $\mathrm{PG}(m-1,q)$ to their product $(x_1y_1, x_1y_2, \ldots, x_ny_m)$ (the x_iy_j are taken in lexicographical order). The image of the Segre map is an algebraic variety called the *Segre variety* and denoted by $\mathcal{S}_{n-1,m-1}$ [14]. The Segre variety $\mathcal{S}_{n-1,m-1}$ has two families of projective subspaces called *rulings*: a family of projective $(n-1)$–dimensional subspaces, say $\mathcal{R}_1$ and a family of projective $(m-1)$–dimensional subspaces, say $\mathcal{R}_2$. Two members in the same ruling are disjoint, a member of $\mathcal{R}_1$ meets an element of $\mathcal{R}_2$ in exactly one point, and each point of $\mathcal{S}_{n-1,m-1}$ is contained in exactly one member of each ruling. The smallest example of Segre variety is $\mathcal{S}_{1,1}$, the hyperbolic quadric $\mathcal{Q}^+(3,q)$ of $\mathrm{PG}(3,q)$. Here, the two rulings are the two reguli of $\mathcal{Q}^+(3,q)$. From [14, Theorem 25.5.14] certain linear sections of dimension $n(n+1)/2-1$ of $\mathcal{S}_{n-1,n-1}$ are Veronese varieties.

The *Veronese variety* of all quadrics of $\mathrm{PG}(n-1,q)$, is the variety $\mathcal{V}$ of $\mathrm{PG}(n(n+1)/2-1,q)$, with parametric equations

$$(x_1^2, x_2^2, \ldots, x_n^2, x_1x_2, x_1x_3, \ldots, x_{n-1}x_n) \tag{2}$$

where $(x_1, x_2, x_3, \ldots, x_n) \in \mathrm{PG}(n-1,q)$. The mapping

$$\mu : \mathrm{PG}(n-1,q) \to \mathrm{PG}(n(n+1)/2-1,q)$$

$$(x_1, x_2, \ldots, x_n) \mapsto (x_1^2, x_2^2, \ldots, x_n^2, x_1x_2, x_1x_3, \ldots, x_{n-1}x_n)$$

is called the *Veronese embedding* of $\mathrm{PG}(n-1,q)$. The variety $\mathcal{V}$ consists of $\theta_{n-1,q}$ points. For more details on Segre varieties and Veronese varieties, see [14].

2.2 Finite classical polar spaces

The finite classical polar spaces are the geometries that are associated with non–degenerate reflexive sesquilinear and non–singular quadratic forms on vector spaces of finite dimension over a finite field. A polar space $\mathcal{P}$ in a projective space $\mathrm{PG}(d,q)$ consists of the projective subspaces of $\mathrm{PG}(d,q)$ that are totally isotropic with relation to a given non–degenerate reflexive sesquilinear form or that are totally singular with relation to a given non–singular quadratic form. The projective space $\mathrm{PG}(d,q)$ is called the ambient projective space of $\mathcal{P}$. Here, the term polar space always refers to a finite classical polar space. A polar space $\mathcal{P}$ is a member of one of the following classes: a symplectic space $\mathcal{W}(2n+1,q)$, a quadric $\mathcal{Q}(2n,q)$, $\mathcal{Q}^+(2n+1,q)$, $\mathcal{Q}^-(2n+1,q)$ or a Hermitian variety $\mathcal{H}(n,q^2)$. A projective subspace M of maximal dimension contained in $\mathcal{P}$ is called a *generator* or a *maximal* of $\mathcal{P}$. The projective dimension of M is said to be the *rank* of $\mathcal{P}$.

A *hyperbolic quadric* $\mathcal{Q}^+(2n-1,q)$ of $\mathrm{PG}(2n-1,q)$, is the set of singular points for some non–degenerate quadratic form of hyperbolic type defined on the underlying vector space. The hyperbolic quadric $\mathcal{Q}^+(2n-1,q)$ has the following number of points:

$$\frac{(q^n-1)(q^{n-1}+1)}{q-1}.$$

The generators of $\mathcal{Q}^+(2n-1,q)$ are $(n-1)$–dimensional projective spaces and the number of generators of $\mathcal{Q}^+(2n-1,q)$ is equal to

$$2\prod_{i=1}^{n-1}(q^i+1).$$

The set of all generators of the hyperbolic quadric $\mathcal{Q}^+(2n-1,q)$ is divided in two distinct subsets of the same size, called *systems of generators* and denoted by $\mathcal{M}_1$ and $\mathcal{M}_2$, respectively.

Lemma 2.1. *Let A and A' two distinct generators of $\mathcal{Q}^+(2n-1,q)$. Then their possible intersections are projective spaces of dimension*

$$\begin{cases} 0, & 2, & 4, & \dots, & n-3 & \textit{if} & A, A' \in \mathcal{M}_i, i=1,2 \\ -1, & 1, & 3, & \dots, & n-2 & \textit{if} & A \in \mathcal{M}_i, A' \in \mathcal{M}_j, i,j \in \{1,2\}, i \neq j \end{cases}$$

if n is odd or

$$\begin{cases} 0, \quad 2, \quad 4, \quad \ldots, \quad n-2 & \text{if} \quad A \in \mathcal{M}_i, A' \in \mathcal{M}_j, i,j \in \{1,2\}, i \neq j \\ -1, \quad 1, \quad 3, \quad \ldots, \quad n-3 & \text{if} \quad A, A' \in \mathcal{M}_i, i = 1,2 \end{cases}$$

if n is even.

We recall the following results, which have been proved in [19, Lemma 3, Corollary 5].

Lemma 2.2. *Let X be a generator of $\mathcal{Q}^+(2n-1,q)$ and let $D(X)$ denote the set of generators of $\mathcal{Q}^+(2n-1,q)$ disjoint from X. Then*

$$|D(X)| = q^{\frac{n(n-1)}{2}}.$$

If X and X' are disjoint generators of $\mathcal{Q}^+(2n-1,q)$, then

$$|D(X) \cap D(X')| = \begin{cases} 0 & \text{if } n \text{ is odd,} \\ q^{\frac{n(n-2)}{4}} \displaystyle\prod_{i=1}^{n/2} (q^{2i-1} - 1) & \text{if } n \text{ is even.} \end{cases}$$

For further details on hyperbolic quadrics we refer to [14].

2.3 Linear representations

Let (V, k) be a non–degenerate formed space with associated polar space $\mathcal{P}$ where V is a $(d+1)$–dimensional vector space over $\mathrm{GF}(q^e)$ and k is a sesquilinear (quadratic) form. The vector space V can be considered as an $(e(d+1))$–dimensional vector space V' over $\mathrm{GF}(q)$ via the inclusion $\mathrm{GF}(q) \subset \mathrm{GF}(q^e)$. Composition of k with the trace map $T : z \in \mathrm{GF}(q^e) \mapsto \sum_{i=1}^{e} z^{q^i} \in \mathrm{GF}(q)$ provides a new form k' on V' and so we obtain a new formed space (V', k'). If our new formed space (V', k') is non–degenerate, then it has an associated polar space $\mathcal{P}'$. The isomorphism types together with various conditions are presented in [18], [21], [12]. Now each point in $\mathrm{PG}(d, q^e)$ corresponds to a 1–dimensional vector space in V, which in turn corresponds to an e–dimensional vector space in V', that is an $(e-1)$–dimensional projective space of $\mathrm{PG}(e(d+1)-1, q)$. Extending this map from points of $\mathrm{PG}(d, q^e)$ to subspaces of $\mathrm{PG}(d, q^e)$, we obtain an injective map from subspaces of $\mathrm{PG}(d, q^e)$ to certain subspaces of $\mathrm{PG}(e(d+1)-1, q)$:

$$\phi : \mathrm{PG}(d, q^e) \to \mathrm{PG}(e(d+1)-1, q).$$

The map ϕ is called the $\mathrm{GF}(q)$–*linear representation* of $\mathrm{PG}(d, q^e)$.

A *partial t–spread* of a projective space $\mathbf{P}$ is a collection $\mathcal{S}$ of mutually disjoint t–dimensional projective subspaces of $\mathbf{P}$. A partial t–spread of $\mathbf{P}$ is said to be a *t–spread* if each point of $\mathbf{P}$ is contained in an element of $\mathbf{P}$. The partial t–spread $\mathcal{S}$ of $\mathbf{P}$ is said to be *maximal*, if there is no partial t–spread $\mathcal{S}'$ of $\mathbf{P}$ containing $\mathcal{S}$ as a proper subset.

The set $\mathcal{D} = \{\phi(P) \mid P \in \mathrm{PG}(d, q^e)\}$ is an example of $(e-1)$–spread of $\mathrm{PG}(e(d+1)-1, q)$, called a *Desarguesian spread* (see [24, Section 25]). The incidence structure whose points are the elements of $\mathcal{D}$ and whose lines are the $(2e-1)$–dimensional projective spaces of $\mathrm{PG}(e(d+1)-1, q)$ joining two distinct elements of $\mathcal{D}$, is isomorphic to $\mathrm{PG}(d, q^e)$. One immediate consequence of the definitions is that the image of the pointset of the original polar space $\mathcal{P}$ is contained in the new polar space $\mathcal{P}'$ (but is not necessarily equal to it).

2.4 A pencil of hyperbolic quadrics in $\mathrm{PG}(2n-1, q)$, n even

The *pencil* of quadrics of $\mathrm{PG}(d, q)$ generated by the quadrics X, X' is the set of quadrics defined by $\lambda X + \mu X'$, where $\lambda, \mu \in \mathrm{GF}(q)$, $(\lambda, \mu) \neq (0, 0)$.

Remark 2.3. If a point $P \in \mathrm{PG}(d, q)$ belongs to two distinct quadrics of a pencil $\mathcal{P}$, then P belongs to every quadric of $\mathcal{P}$. On the other hand, every point of $\mathrm{PG}(d, q)$ is contained in a quadric of $\mathcal{P}$.

Let $\mathcal{Q}^+(n-1, q^2)$ be the hyperbolic quadric of $\mathrm{PG}(n-1, q^2)$, $n \geq 4$ even, with equation

$$X_1 X_{\frac{n+2}{2}} + \ldots + X_{\frac{n}{2}} X_n = 0.$$

From [18, Table 4.3.A], $\phi(\mathcal{Q}^+(n-1, q^2))$ is contained in a hyperbolic quadric $\mathcal{Q}$ of $\mathrm{PG}(2n-1, q)$. Also, from [18, Proposition 4.3.3 i)] the group $K := \mathrm{PGO}^+(n, q^2) \leq \mathrm{PGO}^+(2n-1, q)$ acts irreducibly in $\mathrm{PG}(2n-1, q)$, i.e., it does not fix any non–trivial subspace of $\mathrm{PG}(2n-1, q)$. In particular, points of the quadric $\mathcal{Q}^+(n-1, q^2)$ are mapped, under the $\mathrm{GF}(q)$–linear representation map, to mutually disjoint lines contained in the hyperbolic quadric $\mathcal{Q}$.

Let ω be a primitive element of $\mathrm{GF}(q^2)$ over $\mathrm{GF}(q)$ such that $\omega^2 - \omega - \gamma = 0$, with $\gamma \in \mathrm{GF}(q) \setminus \{0\}$. Then the polynomial $x^2 - x - \gamma$ is irreducible over $\mathrm{GF}(q)$ and $\{1, \omega\}$ is a basis of $\mathrm{GF}(q^2)$ as a vector space over $\mathrm{GF}(q)$. Hence, if $x_i \in \mathrm{GF}(q^2)$ then

$$x_i = y_i + \omega z_i, \tag{3}$$

and $\mathbf{X} = \mathbf{Y} + \omega \mathbf{Z}$, where $\mathbf{X} = (x_1, \ldots, x_n)$, $\mathbf{Y} = (y_1, \ldots, y_n)$, $\mathbf{Z} = (z_1, \ldots, z_n)$.

Set

$$\phi : \mathbf{X} \in \mathrm{PG}(n-1,q^2) \mapsto (\mathbf{Y},\mathbf{Z}) \in \mathrm{PG}(2n-1,q).$$

With this notation, taking into account (3), $\phi(\mathcal{Q}^+(n-1,q^2))$ is contained in two distinct hyperbolic quadrics of $\mathrm{PG}(2n-1,q)$, say $\mathcal{Q}_1$ and $\mathcal{Q}_2$, where

$$\mathcal{Q}_1 : Y_1 Y_{\frac{n+2}{2}} + \ldots + Y_{\frac{n}{2}} Y_n + \gamma (Z_1 Z_{\frac{n+2}{2}} + \ldots + Z_{\frac{n}{2}} Z_n) = 0,$$

$$\mathcal{Q}_2 : Y_1 Z_{\frac{n+2}{2}} + \ldots + Y_{\frac{n}{2}} Z_n + Z_1 Y_{\frac{n+2}{2}} + \ldots + Z_{\frac{n}{2}} Y_n + Z_1 Z_{\frac{n+2}{2}} + \ldots + Z_{\frac{n}{2}} Z_n = 0$$

The hyperbolic quadrics $\mathcal{Q}_1$, $\mathcal{Q}_2$ generate a pencil of $\mathrm{PG}(2n-1,q)$, say $\mathcal{F}$, containing other $q-1$ distinct quadrics, say $\mathcal{Q}_i$, $3 \le i \le q+1$, none of which is degenerate. Indeed, assume that $\mathcal{Q}_i$ is degenerate for some i, then $\mathcal{Q}_i$ is a cone having a distinguished projective subspace of $\mathrm{PG}(2n-1,q)$ as a vertex. Thus K is embedded as a subgroup in the stabilizer of $\mathcal{Q}_i$ in $\mathrm{PGL}(2n,q)$. On the other hand, since any projectivity of $\mathrm{PGL}(2n,q)$ fixing $\mathcal{Q}_i$ has to fix its vertex, we should have that K fixes the vertex of $\mathcal{Q}_i$, contradicting the irreducibility of K. Let $\perp$ be the polarity of $\mathrm{PG}(n-1,q^2)$ associated to $\mathcal{Q}^+(n-1,q^2)$ and let $\perp_i$ be the polarity of $\mathrm{PG}(2n-1,q)$ associated to $\mathcal{Q}_i$, $1 \le i \le q+1$. We need the following lemma.

Lemma 2.4. *Let S be a projective subspace of* $\mathrm{PG}(n-1,q^2)$. *Then* $\phi(S^\perp) = \phi(S)^{\perp_i}$, $1 \le i \le q+1$.

Proof. Let B denote the bilinear form of the n–dimensional $\mathrm{GF}(q^2)$–vector space V underlying $\mathrm{PG}(n-1,q^2)$ associated to $\mathcal{Q}^+(n-1,q^2)$. Let $\mathbf{X},\mathbf{X}' \in V \setminus \{\mathbf{0}\}$. Then $B(\mathbf{X},\mathbf{X}') = B(\mathbf{Y}+\omega\mathbf{Z},\mathbf{Y}'+\omega\mathbf{Z}') = B(\mathbf{Y},\mathbf{Y}') + \omega(B(\mathbf{Z},\mathbf{Y}') + B(\mathbf{Y},\mathbf{Z}')) + w^2 B(\mathbf{Z},\mathbf{Z}') = B(\mathbf{Y},\mathbf{Y}') + \gamma B(\mathbf{Z},\mathbf{Z}') + \omega(B(\mathbf{Z},\mathbf{Y}') + B(\mathbf{Y},\mathbf{Z}') + B(\mathbf{Z},\mathbf{Z}'))$. Let

$$\mathbf{B}_1((\mathbf{Y},\mathbf{Z}),(\mathbf{Y}',\mathbf{Z}')) := B(\mathbf{Y},\mathbf{Y}') + \gamma B(\mathbf{Z},\mathbf{Z}')$$

and

$$\mathbf{B}_2((\mathbf{Y},\mathbf{Z}),(\mathbf{Y}',\mathbf{Z}')) := B(\mathbf{Z},\mathbf{Y}') + B(\mathbf{Y},\mathbf{Z}') + B(\mathbf{Z},\mathbf{Z}').$$

A straightforward computation shows that $\mathbf{B}_i$ is the bilinear form of the $2n$–dimensional $\mathrm{GF}(q)$–vector space underlying $\mathrm{PG}(2n-1,q)$ associated to $\mathcal{Q}_i$, $i = 1,2$. Moreover, $B(\mathbf{X},\mathbf{X}') = 0$ if and only if $\mathbf{B}_1((\mathbf{Y},\mathbf{Z}),(\mathbf{Y}',\mathbf{Z}')) = 0$ and $\mathbf{B}_2((\mathbf{Y},\mathbf{Z}),(\mathbf{Y}',\mathbf{Z}')) = 0$, as required. $\square$

From Lemma 2.4, if g is a generator of $\mathcal{Q}^+(n-1,q^2)$, then $\phi(g)$ is a generator of $\mathcal{Q}_i$, $1 \le i \le q+1$. Hence $\mathcal{Q}_i$ is a non–degenerate quadric of $\mathrm{PG}(2n-1,q)$ of rank $n-1$. Thus $\mathcal{Q}_i$, $1 \le i \le q+1$ is a hyperbolic quadric.

Let $\mathcal{X}$ be the base locus of $\mathcal{F}$. Since the hyperbolic quadrics of $\mathcal{F}$ cover all the points of $\mathrm{PG}(2n-1, q)$, and any two distinct quadrics in $\mathcal{F}$ intersect precisely in $\mathcal{X}$, we have that the following equation holds true:

$$(q+1)(|\mathcal{Q}_1| - |\mathcal{X}|) + |\mathcal{X}| = \theta_{2n-1,q}.$$

It follows that $\mathcal{X}$ consists of

$$\frac{(q^{n-2}+1)(q^n-1)}{q-1}$$

points covered by the lines of $\phi(\mathcal{Q}^+(n-1, q^2))$.

Lemma 2.5. *Let $\mathcal{L}$ be a line–spread of* $\mathrm{PG}(2n-1, q)$ *and let α be a projectivity fixing each line of $\mathcal{L}$. If α fixes a point, then α is the identity.*

Proof. Assume that α fixes the point P. Let ℓ be the unique line of $\mathcal{L}$ containing P. Let Π be a hyperplane containing P and not containing ℓ. Let Σ be the (unique) $(2n-3)$–dimensional projective subspace contained in Π such that $\{r \in \mathcal{L} \mid r \subset \Sigma\}$ is a line–spread of Σ. Then $P \notin \Sigma$. Since Σ is fixed by α and P is fixed by α, we have that Π is fixed by α. Thus every hyperplane through P and not containing ℓ is fixed by α. Let r be a line through P distinct from ℓ. Then there exist $n-2$ distinct hyperplanes Π_i, $1 \leq i \leq n-2$, passing through P, not containing ℓ, such that $\bigcap_{i=1}^{n-2} \Pi_i = r$. We have $\alpha(r) = \alpha(\bigcap_i \Pi_i) = \bigcap_i \alpha(\Pi_i) = \bigcap_i (\Pi_i) = r$ and hence every line through P is fixed by α. Let A be a point not in ℓ, let $m = PA$ and let s be the unique line of $\mathcal{L}$ containing A. Then $A = s \cap m$ and $\alpha(A) = \alpha(s \cap m) = \alpha(s) \cap \alpha(m) = s \cap m = A$ and hence every point not in ℓ is fixed by α. Also, since α fixes the line $s \in \mathcal{L}$ and the point $A \in s$, a similar argument proves that every point not in s is fixed by α. Then every point in ℓ is fixed by α. Since α fixes every point, α is the identity. $\square$

Corollary 2.6. *Let $\mathcal{L}$ be a line–spread of* $\mathrm{PG}(2n-1, q)$*. Let G be the group of projectivities fixing each line of $\mathcal{L}$. Then $|G| \leq q+1$.*

Proof. Suppose that $\alpha_1, \alpha_2 \in G$ and $\alpha_1(P) = \alpha_2(P)$, for some point P. Then $\alpha_1\alpha_2^{-1}(P) = P$. From Lemma 2.5 we have that $\alpha_1\alpha_2^{-1}$ is the identity and so $\alpha_1 = \alpha_2$. Let $P \in \ell \in \mathcal{L}$. Since every projectivity in G fixes ℓ and no two distinct projectivities in G send P to the same point, we have that $|G| \leq |\ell| = q+1$. $\square$

Lemma 2.7. $|G| = q+1$ *and* $G = \{\perp_1\perp_i \mid 1 \leq i \leq q+1\}$.

Proof. The map $\perp_1\perp_i$ is a projectivity fixing each line of $\mathcal{L}$. Indeed, if $P \in \ell \in \mathcal{L}$, then from Lemma 2.4 $\ell^{\perp_i} = \ell^{\perp_j}$. Hence $\ell^{\perp_i} \subset P^{\perp_i}$ and $\ell^{\perp_1} \subset P^{\perp_i}$. It follows that $(P^{\perp_i})^{\perp_1} \in \ell$, i.e. $P^{\perp_1\perp_i} \in \ell$.

Finally, $\perp_1\perp_i = \perp_1\perp_j$ if and only if $i = j$. Thus the set $\{\perp_1\perp_i \mid 1 \leq i \leq q+1\}$ gives rise to $q+1$ distinct projectivities fixing each line of $\mathcal{L}$. By Corollary 2.6, this is the maximum number of such projectivities, so $G = \{\perp_1\perp_i \mid 1 \leq i \leq q+1\}$. □

Proposition 2.8. *There are*

$$2\prod_{i=1}^{n/2-1}(q^{2i}+1)$$

generators belonging to each hyperbolic quadric of the pencil $\mathcal{F}$.

Proof. Let g be a generator belonging to each hyperbolic quadric of the pencil $\mathcal{F}$. Then $g^{\perp_i} = g$, $1 \leq i \leq q+1$ and $g^{\perp_1\perp_i} = g$, $1 \leq i \leq q+1$. It follows that $\{r \in \mathcal{L} \mid r \subset g\}$ is a line–spread of g and therefore there exists a generator m of the quadric $\mathcal{Q}^+(n-1, q^2)$ such that $\phi(m) = g$. Hence, the number of generators belonging to each hyperbolic quadric of the pencil $\mathcal{F}$ equals the number of generators of $\mathcal{Q}^+(n-1, q^2)$. □

Remark 2.9. From the proof of Proposition 2.8, two distinct generators belonging to each hyperbolic quadric of the pencil $\mathcal{F}$ meet in an odd dimensional projective space. Therefore they all belong to the same system of generators with respect to each of the quadrics in $\mathcal{F}$.

Let Σ, Σ' be two disjoint generators of the quadric $\mathcal{Q}(n-1, q^2)$ and let S, S' be their images under the map ϕ, respectively. Hence S and S' are disjoint subspaces belonging to the same system of generators, say $\mathcal{M}_1^i$ of $\mathcal{Q}_i$, $1 \leq i \leq q+1$. Let $\mathcal{G}$ be the set of generators meeting non–trivially both S and S' and belonging to each hyperbolic quadric of the pencil $\mathcal{F}$. We have that $\mathcal{G} \subset \mathcal{M}_1^i$, for every $1 \leq i \leq q+1$ and

$$|\mathcal{G}| = \begin{cases} 2\displaystyle\prod_{i=1}^{n/2-1}(q^{2i}+1) - 2q^{\frac{n(n-2)}{4}} & \text{if } \frac{n}{2} \text{ is odd,} \\ 2\displaystyle\prod_{i=1}^{n/2-1}(q^{2i}+1) - 2q^{\frac{n(n-2)}{4}} + q^{\frac{n(n-4)}{8}}\displaystyle\prod_{i=1}^{n/4}(q^{4i-2}-1) & \text{if } \frac{n}{2} \text{ is even.} \end{cases}$$

Lemma 2.10. *Every $(n-2)$–dimensional projective space contained in $\mathcal{X}$ is contained in a generator belonging to each hyperbolic quadric of the pencil $\mathcal{F}$.*

Proof. Let A be an $(n-2)$–dimensional projective space contained in $\mathcal{X}$ and assume by way of contradiction that there is no generator belonging to each hyperbolic quadric of the pencil $\mathcal{F}$ containing A. Then $A^{\perp_1}$ is an n–dimensional projective space containing two distinct generators, say g_1 and g_2, of $\mathcal{Q}_1$. In particular $g_i \in \mathcal{M}_i^1$, $i = 1, 2$, and $g_1 \cap g_2 = A$.

Since $g_1 \subset \mathcal{Q}_1$ and $g_1 \cap \mathcal{X} = g_1 \cap \mathcal{Q}_2$, we have that $g_1 \cap \mathcal{X}$ is a quadric, say Q, (possibly degenerate) of g_1. Then Q is a quadric of the $(n-1)$–dimensional projective space g_1 containing the $(n-2)$–dimensional projective space A. It follows that either Q coincide with A or Q consists of two distinct $(n-2)$–dimensional projective spaces A, A' and $A \cap A'$ is an $(n-3)$–dimensional projective space.

Let g be a generator belonging to each hyperbolic quadric of the pencil $\mathcal{F}$ such that $g \cap A$ is an r–dimensional projective space. It follows that g and g_1 lie in the same system of generators $\mathcal{M}_1^1$ of $\mathcal{Q}_1$. Then, if r is even, we have that $g \cap g_1$ is an r–dimensional vector space, a contradiction. Analogously, if r is odd, we have that $g \cap g_2$ is an r–dimensional vector space, a contradiction. $\square$

3 The construction

Let $\mathcal{M}_{n\times n}(q)$, $n \geq 4$, be the vector space of all $n \times n$ matrices over the finite field $\mathrm{GF}(q)$. Let $\mathrm{PG}(n^2-1, q)$ be the (n^2-1)–dimensional projective space over $\mathrm{GF}(q)$ where $(X_1, \ldots, X_{n^2})$ are homogeneous projective coordinates. With the identification $a_{i+1,j} = a_{in+j}$, $0 \leq i \leq (n-1)$, $1 \leq j \leq n$, we may associate, up to a non-zero scalar factor, to a matrix $A = (a_{i,j}) \in \mathcal{M}_{n\times n}(q)$ a unique point $P = (a_1, \ldots, a_{n^2}) \in \mathrm{PG}(n^2-1, q)$, and viceversa. In this setting, from [14, Theorem 25.5.7], the Segre variety $\mathcal{S}_{n-1,n-1}$ can be represented by all $n \times n$ matrices of rank 1. Let G' be the subgroup of $\mathrm{PGL}(n^2, q)$ fixing $\mathcal{S}_{n-1,n-1}$. Then $|G'| = 2|\mathrm{PGL}(n, q)|$. The group G' contains a subgroup of index two, say G, isomorphic to $\mathrm{PGL}(n, q) \times \mathrm{PGL}(n, q)$ and every element in G has a matrix representation of the form $A \otimes B$, where $A, B \in \mathrm{GL}(n, q)$ [14, Theorem 25.5.13]. Here $\otimes$ denotes the Kronecker product. In this context the subspace of all symmetric matrices of $\mathcal{M}_{n\times n}(q)$ is represented by the $(n(n+1)/2-1)$–dimensional projective subspace Γ of $\mathrm{PG}(n^2-1, q)$ defined by the following equations:

$$X_{in+j} = X_{(j-1)n+i+1}, \quad 0 \leq i \leq n-2, i+2 \leq j \leq n.$$

In particular Γ meets the Segre variety $\mathcal{S}_{n-1,n-1}$ in a Veronese variety $\mathcal{V}$ [14, Theorem 25.5.8].

Remark 3.1. The subgroup of G' fixing $\mathcal{V}$ contains a subgroup, say H, isomorphic to $\mathrm{PGL}(n,q)$ and every element in H has a matrix representation of the form $A \otimes A$, where $A \in \mathrm{GL}(n,q)$. The group H leaves invariant an $(n(n-1)/2-1)$–dimensional projective subspace Γ', which corresponds to the subspace of all skew–symmetric matrices of $\mathcal{M}_{n\times n}(q)$. In particular, Γ' is either contained in or disjoint to Γ according as q is even or odd, respectively. In any case Γ' is disjoint from $\mathcal{S}_{n-1,n-1}$.

In $\mathrm{PG}(n-1,q^n)$ consider a q–order subgeometry $\Sigma := \mathrm{PG}(n-1,q)$. Let $\bar{C}$ a Singer cycle of $\mathrm{GL}(n,q)$ and let $C \in \mathrm{PGL}(n,q)$ be the corresponding collineation of $\mathrm{PG}(n-1,q)$. Then $\langle C\rangle$ is a Singer cyclic group of order $\theta_{n-1,q} = (q^n-1)/(q-1)$. The group $\langle C\rangle$ fixes n points in general position, say $P_1,\ldots,P_n$ and the hyperplanes $\bar{\Pi}_i := \langle P_1,\ldots,P_{i-1},P_{i+1},\ldots,P_n\rangle$. Also it partitions $\mathrm{PG}(n-1,q^n)\setminus\bigcup_i\bar{\Pi}_i$ into $(q-1)(q^n-1)^{n-2}$ q–order subgeometries, see [2].

By considering the $\mathrm{GF}(q)$–linear representation of $\mathrm{PG}(n-1,q^n)$, a point of $\mathrm{PG}(n-1,q^n)$ becomes an $(n-1)$–dimensional projective subspace π which is a member of a Desarguesian spread of a $\mathrm{PG}(n^2-1,q)$. In particular points of a q–order subgeometry of $\mathrm{PG}(n-1,q^n)$ become maximal spaces of a ruling of a Segre variety $\mathcal{S}_{n-1,n-1}$ of $\mathrm{PG}(n^2-1,q)$, see [22]. From the discussion above, it follows that in $\mathrm{PG}(n^2-1,q)$ we see a set consisting of n (n^2-n-1)–dimensional projective subspaces $\Pi_i := \phi(\bar{\Pi}_i)$, $i=1,\ldots,n$ and a partition, say $\mathcal{P}$, of $\mathrm{PG}(n^2-1,q)\setminus\bigcup_i(\Pi_i)$ into $(q-1)(q^n-1)^{n-2}$ Segre varieties $\mathcal{S}_{n-1,n-1}$.

Proposition 3.2. *There exists an (n^2-n-1)–dimensional projective space that is disjoint from $\mathcal{S}_{n-1,n-1}$ and contains Γ'.*

Proof. From [16], $\bar{C}$ is conjugate in $\mathrm{GL}(n,q^n)$ to a diagonal matrix D

$$D = diag(\omega,\omega^q,\ldots\omega^{q^{n-1}}),$$

for some primitive element ω of $\mathrm{GF}(q^n)$, i.e., there exists a matrix $E \in \mathrm{GL}(n,q^n)$ with $E^{-1}\bar{C}E = D$. Then $D\otimes D$ is the block diagonal matrix

$$diag(\omega D,\omega^q D,\ldots,\omega^{q^{n-1}}D)$$

and since $\omega^{q^n}=\omega$, it has exactly $n(n+1)/2$ distinct entries. It follows that $D\otimes D$ has exactly $n(n+1)/2$ distinct eigenvalues. The projectivity induced by $\bar{C}\otimes\bar{C}$ has order $\theta_{n-1,q}$, is contained in G and fixes $\mathcal{V}$, see Remark (3.1). Since

$$(E\otimes E)^{-1}(\bar{C}\otimes\bar{C})(E\otimes E) = D\otimes D,$$

the projectivity induced by $D \otimes D$ stabilizes the Segre variety $\hat{\mathcal{S}}_{n-1,n-1}$ corresponding to $\mathcal{S}_{n-1,n-1}$. The collineation group, say J, associated to $\langle D \otimes D \rangle$, has order $\theta_{n-1,q}$. It fixes the q–order subgeometry Π of $\mathrm{PG}(n^2-1, q^n)$ whose points are:

$$(\alpha_1, \ldots, \alpha_n, \alpha_n^q, \alpha_1^q, \ldots, \alpha_{n-1}^q, \alpha_{n-1}^{q^2}, \alpha_n^{q^2}, \ldots, \alpha_{n-2}^{q^2}, \ldots, \alpha_2^{q^{n-1}}, \ldots, \alpha_1^{q^{n-1}}),$$

where $\alpha_i \in \mathrm{GF}(q^n)$, $1 \leq i \leq n$, $(\alpha_1, \ldots, \alpha_n) \neq (0, \ldots, 0)$, the Segre variety $\hat{\mathcal{S}}_{n-1,n-1}$ and the Veronese variety $\hat{\mathcal{V}} = \hat{\Gamma} \cap \hat{\mathcal{S}}_{n-1,n-1}$. Furthermore the group J fixes the following n $(n-1)$–dimensional projective subspaces of Π:

$$\mathcal{X}_1 = \langle U_{(a-1)n+a} \rangle, \;\; 1 \leq a \leq n,$$

$$\mathcal{X}_k = \langle U_{(a_1-k)n+a_1}, U_{(n-k)n+a_2(n+1)} \rangle, \;\; k \leq a_1 \leq n, 1 \leq a_2 \leq k-1, 2 \leq k \leq n,$$

where U_i denotes the point with coordinates $(0, \ldots, 0, 1, 0, \ldots, 0)$, with 1 in the $i-$th position.

Since $D \otimes D$ has $n(n+1)/2$ distinct eigenvalues, every J–orbit of a point of Π whose coordinates are all non–zero generates an $(n(n+1)/2-1)$–projective subspace of Π. As a consequence, since $\hat{\Gamma}'$ is an $(n(n-1)/2-1)$–dimensional projective subspace fixed by J, $\hat{\Gamma}'$ is contained in $\bigcup_i \hat{\Pi}_i$. By way of contradiction, assume that $\hat{\Gamma}'$ is not contained in $\hat{\Pi}_i$ for every i. Then, since $\hat{\Gamma}' \cap \bigcup_i \hat{\Pi}_i = \bigcup_i (\hat{\Gamma}' \cap \hat{\Pi}_i)$, we can find $P, Q \in \hat{\Gamma}'$ such that $P \in \hat{\Pi}_i$ and $P \notin \hat{\Pi}_k$ for every $k \neq i$, $Q \in \hat{\Pi}_j$ and $Q \notin \hat{\Pi}_k$ for every $k \neq j$, with $i \neq j$. It follows that the line $PQ \subset \hat{\Gamma}'$ but $PQ \notin \bigcup_i \hat{\Pi}_i$. A contradiction. $\square$

Let $\mathcal{Y}$ denote the (n^2-n-1)–dimensional projective subspace that is disjoint from $\mathcal{S}_{n-1,n-1}$ and contains Γ'.

We denote by $\mathcal{A}$ the set consisting of the $q^{n(n-1)/2}$ matrices corresponding to the points of Γ' (together with the zero matrix). Since the Segre variety $\mathcal{S}_{n-1,n-1}$ can be represented by all $n \times n$ matrices of rank 1 [14, Theorem 25.5.7] and $\mathcal{Y}$ is disjoint from $\mathcal{S}_{n-1,n-1}$, we have that the set $\mathcal{M}$, consisting of the q^{n^2-n} matrices corresponding to the points of $\mathcal{Y}$ (together with the zero matrix), form a linear $(n, n, n-1)$ MRD code. Indeed, any matrix in $\mathcal{M}$ has rank at least two.

From [25] we recall the following *lifting process* for MRD codes. Let A be an $n \times n$ matrix over $\mathrm{GF}(q)$, and let I_n be the $n \times n$ identity matrix. The rows of the $n \times 2n$ matrix $(I_n|A)$ can be viewed as coordinates of points in general position of an $(n-1)$–dimensional projective space of $\mathrm{PG}(2n-1, q)$. This subspace is denoted by $L(A)$. Hence the matrix A can be *lifted* to a subspace $L(A)$. From [25], a q-ary $(n, n, n-1)$ MRD lifts to a q-ary $(2n, q^{n^2-n}, 4; n)$

constant–dimension subspace code. A constant–dimension code such that all its codewords are lifted codewords of an MRD code is called a *lifted MRD code.* Let $\mathcal{L}_1 = \{L(A) \mid A \in \mathcal{M}\}$ be the constant–dimension code obtained by lifting the $(n, n, n-1)$ MRD code contructed above. Then $\mathcal{L}_1$ consists of $(n-1)$–dimensional projective spaces mutually intersecting in at most an $(n-3)$–dimensional projective space. In particular, members of $\mathcal{L}_1$ are disjoint from the special $(n-1)$–dimensional projective space $S = \langle U_{n+1}, \ldots, U_{2n}\rangle$ and therefore every $(n-2)$–dimensional projective space covered by an element of $\mathcal{L}_1$ is disjoint from S. Moreover, from [15, Lemma 6], every $(n-2)$–dimensional projective space in $\mathrm{PG}(2n-1, q)$ disjoint from S is covered by a member of $\mathcal{L}_1$ exactly once. We denote by S' the special $(n-1)$–dimensional projective space $\langle U_1, \ldots, U_n\rangle$.

From [10] it is known that a linear $(n, n, n-1)$ MRD code contains an $(n, n, 2, r)$ CRC of size

$$\begin{bmatrix} n \\ r \end{bmatrix}_q \sum_{j=2}^{r} (-1)^{(r-j)} \begin{bmatrix} r \\ j \end{bmatrix}_q q^{\binom{r-j}{2}} (q^{n(j-1)} - 1), \tag{4}$$

consisting of all matrices of the linear $(n, n, n-1)$ MRD code having rank r.

Let $\mathcal{C}_r$ denote the $(n, n, 2, r)$ CRC of size (4) contained in $\mathcal{Y}$. Let A be an element of $\mathcal{C}_r$, $2 \le r \le (n-2)$. As in the discussion above, the rows of the $n \times 2n$ matrix $(A|I_n)$ can be viewed as coordinates of points in general position of an $(n-1)$–dimensional projective space of $\mathrm{PG}(2n-1, q)$. This subspace is denoted by $L'(A)$. The subspace $L'(A)$ is disjoint from S' and meets S in an $(n-r-1)$–dimensional projective space. Let $\mathcal{L}_r = \{L'(A) \mid A \in \mathcal{C}_r\}$ be the constant–dimension code obtained by lifting the $(n, n, 2, r)$ CRC codes $\mathcal{C}_r$, $2 \le r \le (n-2)$ constructed above.

Lemma 3.3. *The set* $\bigcup_{i=1}^{n-2} \mathcal{L}_i$ *is a* $(2n, M, 4; n)_q$ *constant–dimension subspace code, where*

$$M = q^{n^2-n} + \sum_{r=2}^{n-2} \begin{bmatrix} n \\ r \end{bmatrix}_q \sum_{j=2}^{r} (-1)^{(r-j)} \begin{bmatrix} r \\ j \end{bmatrix}_q q^{\binom{r-j}{2}} (q^{n(j-1)} - 1).$$

Proof. By construction, every $(n-2)$–dimensional projective space contained in $L'(A)$ meets S in at least a point and is disjoint from S'. If $A_1 \in \mathcal{C}_{r_1}$, $A_2 \in \mathcal{C}_{r_2}$, then $rg(A_1 - A_2) \ge 2$ and $rg\begin{pmatrix} A_1 & I_n \\ A_2 & I_n \end{pmatrix} = n + rg(A_1 - A_2) \ge n+2$. It follows that $L'(A_1)$ meets $L'(A_2)$ in at most an $(n-3)$–dimensional projective space. We may conclude by observing that every

$(n-2)$–dimensional projective space covered by a member of $\mathcal{L}_1 \cup (\bigcup_{i=2}^{n-2} \mathcal{L}_i)$ is covered by exactly one element of $\mathcal{L}_1 \cup (\bigcup_{i=2}^{n-2} \mathcal{L}_i)$, as required. $\square$

Now, we introduce the non–degenerate hyperbolic quadric $\mathcal{Q}$ of $\mathrm{PG}(2n-1, q)$ having the following equation:

$$X_1X_{n+1} + X_2X_{n+2} + \ldots + X_nX_{2n} = 0.$$

The subspaces S and S' are maximals of $\mathcal{Q}$. They belong either to the same system of maximals of $\mathcal{Q}$ or to different systems, according as n is even or odd, respectively. Let $\mathcal{M}_1$ be the system of maximals of $\mathcal{Q}$ containing S and let $D(X)$ and $I(X)$ denote the set of maximals in $\mathcal{M}_1$ disjoint from the maximal X or meeting non–trivially X, respectively.

Lemma 3.4. *Let A be a skew–symmetric matrix in $\mathcal{M}_{n\times n}(q)$. Then $L(A)$ (resp. $L'(A)$) is a maximal of $\mathcal{Q}$ disjoint from S (resp. S').*

Proof. From the definitions of $L(A)$ and S, we have that $L(A) = \langle (I|A) \rangle$ and $S = \langle (0_n|I_n) \rangle$. Since the rank of the matrix $\begin{pmatrix} I_n & A \\ 0_n & I_n \end{pmatrix}$ is $2n$, it follows that $L(A)$ is disjoint from S. The matrix of the bilinear form associated to the quadric $\mathcal{Q}$ is $\begin{pmatrix} 0_n & I_n \\ I_n & 0_n \end{pmatrix}$. Then $L(A)$ is contained in $\mathcal{Q}$ if and only if

$$(I_n|A) \begin{pmatrix} 0_n & I_n \\ I_n & 0_n \end{pmatrix} (I_n|A)^t = 0,$$

if and only if $A + A^t = 0$. $\square$

Remark 3.5. Since the number of maximals of $\mathcal{Q}$ disjoint from S equals $|\mathcal{A}| = q^{n(n-1)/2}$ [19, Lemma 3], we have that each such a maximal is of the form $L(A)$, for some $A \in \mathcal{A}$. Notice that, if $A \in \mathcal{A}$, then $L(A)$ belongs either to $\mathcal{M}_1$ or to $\mathcal{M}_2$, according as n is even or odd, respectively.

3.1 n even

Assume that n is even. In this case we have that

$$\mathcal{M}_1 = D(S) \cup (D(S') \cap I(S)) \cup (I(S) \cap I(S')),$$

where $D(S)$, $D(S') \cap I(S)$ and $I(S) \cap I(S')$ are trivially intersecting sets. On the other hand, a maximal $L'(A)$ in $D(S')$ is disjoint from S if and only if A is a skew–symmetric matrix of rank n. Therefore, the number of skew–symmetric matrices of rank n is equal to $|D(S)\cap D(S')|$. It follows that

$$|D(S')\cap I(S)| = |D(S)| - |D(S)\cap D(S')| = q^{\frac{n(n-1)}{2}} - q^{\frac{n(n-2)}{4}}\prod_{i=1}^{n/2}(q^{2i-1}-1)$$

and

$$|I(S)\cap I(S')| = |\mathcal{M}_1| - 2q^{\frac{n(n-1)}{2}} + q^{\frac{n(n-2)}{4}}\prod_{i=1}^{n/2}(q^{2i-1}-1).$$

Since $\mathcal{A}\subset\mathcal{M}$, we have that $D(S)\subset\mathcal{L}_1$. Moreover, every element $g\in D(S')\cap I(S)$ is of the form $L'(A)$ for some skew–symmetric matrix A having rank r, with $2\le r\le n-2$. Hence $g\in\mathcal{L}_r$.

Lemma 3.6. *The set* $\bigcup_{i=1}^{n-2}\mathcal{L}_i\cup(I(S)\cap I(S'))$ *is a* $(2n, M, 4; n)_q$ *constant–dimension subspace code, where*

$$\begin{aligned} M &= q^{n^2-n} + \sum_{r=2}^{n-2}\begin{bmatrix} n \\ r \end{bmatrix}_q \sum_{j=2}^{r}(-1)^{(r-j)}\begin{bmatrix} r \\ j \end{bmatrix}_q q^{\binom{r-j}{2}}(q^{n(j-1)}-1) \\ &\quad + \prod_{i=1}^{n-1}(q^i+1) - 2q^{\frac{n(n-1)}{2}} + q^{\frac{n(n-2)}{4}}\prod_{i=1}^{n/2}(q^{2i-1}-1). \end{aligned}$$

Proof. Notice that each member of $\mathcal{L}_1$ (resp. $\mathcal{L}_r$, $2\le r\le n-2$) is disjoint from S (resp. S'), whereas each member of $I(S)\cap I(S')$ has at least a line in common with both S and S'. Hence $I(S)\cap I(S')$ is disjoint from $\bigcup_{i=1}^{n-2}\mathcal{L}_i$. On the other hand, each $(n-2)$–dimensional projective space covered by a member of $\mathcal{L}_1$ (resp. $\mathcal{L}_r$, $2\le r\le n-2$) is disjoint from S (resp. S'), whereas each $(n-2)$–dimensional projective space covered by a member of $I(S)\cap I(S')$ has at least a point in common with both S and S'. Then $(\bigcup_{i=1}^{n-2}\mathcal{L}_i)\cup(I(S)\cap I(S'))$ is a set of $(n-1)$–dimensional projective spaces mutually intersecting in at most an $(n-3)$–dimensional projective space. $\square$

From Section 2.4, there exists a pencil $\mathcal{F}$ comprising $q+1$ hyperbolic quadrics $\mathcal{Q}_i$, $1\le i\le q+1$ of $\mathrm{PG}(2n-1,q)$ distinct from $\mathcal{Q}=\mathcal{Q}_1$. Let $I_i(X)$ denote the set of maximals in $\mathcal{M}_1^i$ meeting non–trivially X, $2\le i\le(q+1)$ and, according to the notation of Remark 2.9, let $\mathcal{G}=\bigcap_{i=2}^{q+1}(I_i(S)\cap I_i(S'))\cap(I(S)\cap I(S'))$.

Lemma 3.7. *The set* $(\bigcup_{i=1}^{n-2}\mathcal{L}_i)\cup(\bigcup_{i=2}^{q+1}(I_i(S)\cap I_i(S')))\cup(I(S)\cap I(S'))$ *is a* $(2n, M, 4; n)_q$ *constant–dimension subspace code, where*

$$\begin{aligned} M &= q^{n^2-n}+\sum_{r=2}^{n-2}\begin{bmatrix} n\\ r\end{bmatrix}_q\sum_{j=2}^{r}(-1)^{(r-j)}\begin{bmatrix} r\\ j\end{bmatrix}_q q^{\binom{r-j}{2}}(q^{n(j-1)}-1)\\ &\quad +(q+1)\left(\prod_{i=1}^{n-1}(q^i+1)-2q^{\frac{n(n-1)}{2}}+q^{\frac{n(n-2)}{4}}\prod_{i=1}^{n/2}(q^{2i-1}-1)\right)-q|\mathcal{G}|. \end{aligned}$$

Proof. From Remark (2.3), a maximal of a quadric of the pencil $\mathcal{F}$ belongs either to one or to all quadrics of the pencil $\mathcal{F}$. Then, from Section (2.4), we have that

$$\begin{aligned} |\bigcup_{i=2}^{q+1}(I_i(S)\cap I_i(S'))| &= q(|I(S)\cap I(S')|-|\mathcal{G}|)\\ &= q\left(|\mathcal{M}_1|-2q^{\frac{n(n-1)}{2}}+q^{\frac{n(n-2)}{4}}\prod_{i=1}^{n/2}(q^{2i-1}-1)-|\mathcal{G}|\right). \end{aligned}$$

Each $(n-2)$–dimensional projective space covered by a member of $\mathcal{L}_1$ (resp. $\mathcal{L}_r$, $2\le r\le n-2$) is disjoint from S (resp. S'), whereas each $(n-2)$–dimensional projective space covered by a member of $\bigcup_{i=2}^{q+1}(I_i(S)\cap I_i(S'))\cup(I(S)\cap I(S'))$ has at least a point in common with both S and S'. Also, since two distinct elements of $I_i(S)\cap I_i(S')$ are maximals of a distinguished quadric of the pencil $\mathcal{F}$ contained in the same system, they have at most an $(n-3)$–dimensional projective space in common. On the other hand, let $g_i\in I_i(S)\cap I_i(S')$ and $g_j\in I_j(S)\cap I_j(S')$, $i\ne j$, and assume that $g_i\cap g_j=A$, where A is an $(n-2)$–dimensional projective space. Then A is contained in the base locus $\mathcal{X}$ of the pencil $\mathcal{F}$ and, from Lemma 2.10, there exists a maximal g belonging to each quadric of the pencil $\mathcal{F}$ containing A. Hence $g, g_i\in\mathcal{M}_1^i$ and $g\cap g_i=A$, a contradiction. It follows that $(\bigcup_{i=1}^{n-2}\mathcal{L}_i)\cup(\bigcup_{i=2}^{q+1}(I_i(S)\cap I_i(S')))\cup(I(S)\cap I(S'))$ is a set of $(n-1)$–dimensional projective spaces mutually intersecting in at most an $(n-3)$–dimensional projective space, as required. $\square$

We are ready to prove the main theorem of this Section.

Theorem 3.8. *If n is even, there exists a* $(2n, M, 4; n)_q$ *constant–dimension* *subspace code, where*

$$\begin{aligned} M &= q^{n^2-n} + \sum_{r=2}^{n-2} \begin{bmatrix} n \\ r \end{bmatrix}_q \sum_{j=2}^{r} (-1)^{(r-j)} \begin{bmatrix} r \\ j \end{bmatrix}_q q^{\binom{r-j}{2}} (q^{n(j-1)} - 1) \\ &+ (q+1) \left(\prod_{i=1}^{n-1} (q^i + 1) - 2q^{\frac{n(n-1)}{2}} + q^{\frac{n(n-2)}{4}} \prod_{i=1}^{n/2} (q^{2i-1} - 1) \right) \\ &- q|\mathcal{G}| + \begin{bmatrix} \frac{n}{2} \\ 1 \end{bmatrix}_{q^2} \left(\begin{bmatrix} \frac{n}{2} \\ 1 \end{bmatrix}_{q^2} - 1 \right) + 1. \end{aligned}$$

Proof. The set $\mathcal{G}$ contains a subset $\mathcal{D}$ consisting of $\theta_{(n-2)/2,q^2}$ generators belonging to each hyperbolic quadric of the pencil $\mathcal{F}$ such that every element in $\mathcal{D}$ meets S in a line and S' in an $(n-3)$–dimensional projective space and the set $\mathcal{D}_S = \{A \cap S \mid A \in \mathcal{D}\}$ is a Desarguesian line–spread of S. In other words $\mathcal{D}_S = \{\phi(P) \mid P \in \Sigma\}$. On the other hand, the set $\mathcal{D}_{S'} = \{A \cap S' \mid A \in \mathcal{D}\}$ is a set of $(n-3)$–dimensional projective space mutually intersecting in an $(n-5)$–dimensional projective space. In particular for a fixed line $\ell \in \mathcal{D}_S$ there exists a unique element in $\mathcal{D}_{S'}$, say A_ℓ, such that $\langle \ell, A_\ell \rangle$ is in $\mathcal{D}$, and viceversa. Furthermore, if $\ell \in \mathcal{D}_S$ and $B \in \mathcal{D}_{S'} \setminus \{A_\ell\}$, then $\langle \ell, B \rangle$ is an $(n-1)$–dimensional projective space meeting a hyperbolic quadric of the pencil $\mathcal{F}$ in a cone having as vertex $A_\ell \cap B$ and as base a $\mathcal{Q}^+(3,q)$ containing ℓ. Notice that such a cone meets a generator of a hyperbolic quadric of the pencil $\mathcal{F}$ in at most an $(n-3)$–dimensional projective space. Let $\mathcal{D}'$ be the set of $(n-1)$–dimensional projective spaces of the form $\langle \ell, B \rangle$, where $\ell \in \mathcal{D}_S$ and $B \in \mathcal{D}_{S'} \setminus \{A_\ell\}$. Then $\mathcal{D}'$ is disjoint from $\mathcal{D}$. Also $|\mathcal{D}'| = \theta_{(n-2)/2,q^2}(\theta_{(n-2)/2,q^2} - 1)$. From the discussion above, taking into account Lemma 3.6 and Lemma 3.7, we have that $(\bigcup_{i=1}^{n-2} \mathcal{L}_i) \cup (\bigcup_{i=2}^{q+1} (I_i(S) \cap I_i(S'))) \cup (I(S) \cap I(S')) \cup \mathcal{D}' \cup \{S\}$ is a set of $(n-1)$–dimensional projective spaces mutually intersecting in at most an $(n-3)$–dimensional projective space, as required. $\square$

3.2 n odd

Assume that n is odd. In this case $|D(S)| = 0$, then

$$\mathcal{M}_1 = (D(S') \cap I(S)) \cup (I(S) \cap I(S')),$$

where $D(S') \cap I(S)$, $D(S')$ are trivially intersecting sets and $|D(S') \cap I(S)| = |D(S')| = q^{\frac{n(n-1)}{2}}$. It follows that $|I(S) \cap I(S')| = |\mathcal{M}_1| - q^{\frac{n(n-1)}{2}}$.

If we denote by $\mathcal{I}$ the subset of $I(S) \cap I(S')$ consisting of maximals intersecting S in exactly a point, we have the following.

Lemma 3.9.

$$|\mathcal{I}| = \theta_{n-1,q} \left(q^{\frac{(n-1)(n-2)}{2}} - q^{\frac{(n-1)(n-3)}{4}} \prod_{i=1}^{n-1/2} (q^{2i-1} - 1) \right)$$

Proof. Let P be a point of S. If $\perp$ is the polarity of $\mathrm{PG}(2n-1, q)$ associated with $\mathcal{Q}$, then $P^{\perp}$ is a hyperplane meeting $\mathcal{Q}$ in a cone having as vertex the point P and as base a hyperbolic quadric $\mathcal{Q}^+(2n-3, q)$. Both $S \cap \mathcal{Q}^+(2n-3, q)$ and $S' \cap \mathcal{Q}^+(2n-3, q)$ are maximals of $\mathcal{Q}^+(2n-3, q)$. It follows that the number of maximals of $I(S) \cap I(S')$ intersecting S exactly in P equals the number of maximals of $\mathcal{Q}^+(2n-3, q)$ disjoint from S and meeting S' non–trivially. $\square$

Lemma 3.10. *The set* $(\bigcup_{i=1}^{n-2} \mathcal{L}_i) \cup (I(S) \cap I(S') \setminus \mathcal{I}) \cup \{S\}$ *is a* $(2n, M, 4; n)_q$ *constant–dimension subspace code, where*

$$\begin{aligned} M &= q^{n^2-n} + \sum_{r=2}^{n-2} \begin{bmatrix} n \\ r \end{bmatrix}_q \sum_{j=2}^{r} (-1)^{(r-j)} \begin{bmatrix} r \\ j \end{bmatrix}_q q^{\binom{r-j}{2}} (q^{n(j-1)} - 1) + \prod_{i=1}^{n-1} (q^i + 1) \\ &\quad - q^{\frac{n(n-1)}{2}} - \theta_{n-1,q} \left(q^{\frac{(n-1)(n-2)}{2}} - q^{\frac{(n-1)(n-3)}{4}} \prod_{i=1}^{n-1/2} (q^{2i-1} - 1) \right) + 1. \end{aligned}$$

Proof. From Lemma 3.3, $\bigcup_{i=1}^{n-2} \mathcal{L}_i$ has the required property. Moreover, each member of $\mathcal{L}_1$ (resp. $\mathcal{L}_r$, $2 \le r \le n-2$) is disjoint from S (resp. S'), whereas, by construction, each member of $I(S) \cap I(S') \setminus \mathcal{I}$ has at least a line in common with S' and at least a plane in common with S. Hence $I(S) \cap I(S') \setminus \mathcal{I}$ is disjoint from $\bigcup_{i=1}^{n-2} \mathcal{L}_i$. On the other hand, each $(n-2)$–dimensional projective space covered by a member of $\mathcal{L}_1$ (resp. $\mathcal{L}_r$, $2 \le r \le n-2$) is disjoint from S (resp. S'), whereas each $(n-2)$–dimensional projective space covered by a member of $I(S) \cap I(S') \setminus \mathcal{I}$ has at least a point in common with S' and a line in common with S. Also, since two distinct elements of $(I(S) \cap I(S') \setminus \mathcal{I}) \cup \{S\}$ are maximals of $\mathcal{Q}$ contained in the same system, they have at most an $(n-3)$–dimensional projective space in common. It follows that $(\bigcup_{i=1}^{n-2} \mathcal{L}_i) \cup (I(S) \cap I(S') \setminus \mathcal{I}) \cup \{S\}$ is a set of $(n-1)$–dimensional projective spaces mutually intersecting in at most an $(n-3)$–dimensional projective space, as required. $\square$

From [1, Theorem 4.6] a partial line–spread of $\mathrm{PG}(n-1,q)$, $n \geq 5$ odd, has size at most $y := q^{n-2} + q^{n-4} + \ldots + q^3 + 1$ and actually examples of this size exist. We are ready to prove the main theorem of this Section.

Theorem 3.11. *If n is odd, there exists a $(2n, M, 4; n)_q$ constant–dimension subspace code, where*

$$\begin{aligned} M &= q^{n^2-n} + \sum_{r=2}^{n-2} \begin{bmatrix} n \\ r \end{bmatrix}_q \sum_{j=2}^{r} (-1)^{(r-j)} \begin{bmatrix} r \\ j \end{bmatrix}_q q^{\binom{r-j}{2}} (q^{n(j-1)} - 1) + \prod_{i=1}^{n-1} (q^i + 1) \\ &\quad - q^{\frac{n(n-1)}{2}} - \theta_{n-1,q} \left(q^{\frac{(n-1)(n-2)}{2}} - q^{\frac{(n-1)(n-3)}{4}} \prod_{i=1}^{n-1/2} (q^{2i-1} - 1) \right) \\ &\quad + y(y-1) + 1. \end{aligned}$$

Proof. Let $\mathcal{S}$ be a partial line–spread of S such that $|\mathcal{S}| = y$. Consider the set $\mathcal{D}$ consisting of y generators of $\mathcal{Q}$, such that every element in $\mathcal{D}$ is generated by a line ℓ of $\mathcal{S}$ and S' and the $(n-3)$–dimensional projective space $\ell^{\perp} \cap S'$. The set $\mathcal{D}_{S'} = \{A \cap S' \mid A \in \mathcal{D}\}$ is a set of $(n-3)$–dimensional projective space of S' mutually intersecting in an $(n-5)$–dimensional projective space. In particular for a fixed line $\ell \in \mathcal{S}$ there exists a unique element in $\mathcal{D}_{S'}$, say A_ℓ, such that $\langle \ell, A_\ell \rangle$ is in $\mathcal{D}$, and viceversa. Furthermore, if $\ell \in \mathcal{S}$ and $B \in \mathcal{D}_{S'} \setminus \{A_\ell\}$, then $\langle \ell, B \rangle$ is an $(n-1)$–dimensional projective space meeting $\mathcal{Q}$ in a cone having as vertex $A_\ell \cap B$ and as base a $\mathcal{Q}^+(3,q)$ containing ℓ. Notice that such a cone meets a generator of $\mathcal{Q}$ in at most an $(n-3)$–dimensional projective space. Let $\mathcal{D}'$ be the set of $(n-1)$–dimensional projective spaces of the form $\langle \ell, B \rangle$, where $\ell \in \mathcal{S}$ and $B \in \mathcal{D}_{S'} \setminus \{A_\ell\}$. Then $|\mathcal{D}'| = y(y-1)$. From the discussion above, taking into account Lemma 3.10, we have that $(\bigcup_{i=1}^{n-2} \mathcal{L}_i) \cup (I(S) \cap I_i(S') \setminus \mathcal{I}) \cup \mathcal{D}' \cup \{S\}$ is a set of $(n-1)$–dimensional projective spaces mutually intersecting in at most an $(n-3)$–dimensional projective space, as required. $\square$

4 The case of $\mathrm{PG}(7,q)$

In this section we specialize to the case of the triality quadric $\mathcal{Q}^+(7,q)$. We will denote by $\perp$ the polarity of $\mathrm{PG}(7,q)$ induced by $\mathcal{Q}^+(7,q)$.

Let us denote by $\mathcal{M}_1$ and $\mathcal{M}_2$ the two systems of generators of $\mathcal{Q}^+(7,q)$, by $\mathcal{L}$ the set of lines of $\mathcal{Q}^+(7,q)$ and by $\mathcal{P}$ the set of points of $\mathcal{Q}^+(7,q)$. Then the rank 4 incidence geometry $\Omega = (\mathcal{P}, \mathcal{L}, \mathcal{M}_1, \mathcal{M}_2)$ can be attached to $\mathcal{Q}^+(7,q)$ as follows. An element $G_1 \in \mathcal{M}_1$ is said to be incident with an element $G_2 \in \mathcal{M}_2$ if and only if the intersection $G_1 \cap G_2$ is a plane of $\mathcal{Q}^+(7,q)$. Incidence between other elements is symmetrized containment. Every permutation of the set $\{\mathcal{P}, \mathcal{M}_1, \mathcal{M}_2\}$ defines a geometry Ω' isomorphic to Ω and hence the automorphism groups of Ω and Ω' are isomorphic.

A *triality* of the geometry Ω is a map τ:

$$\tau : \mathcal{L} \to \mathcal{L}, \mathcal{P} \to \mathcal{M}_1, \mathcal{M}_1 \to \mathcal{M}_2, \mathcal{M}_2 \to \mathcal{P}$$

preserving the incidence in Ω and such that τ^3 is the identity.

Here, we will improve, in the case $n = 4$, the result established in Theorem 3.8, which yields an $(8, M, 4; 4)_q$ CDC, say Z, where

$$M = q^{12} + (q^2-1)(q^2+1)^2(q^2+q+1) + (q^3+3q^2+q+1)(q^2+1) + 1,$$

by considering some more suitable projective 3–spaces (solids). Recall, from Section 3.1, that the solids of Z meeting both S and S' are generators of some hyperbolic quadric of the pencil $\mathcal{F}$. In this case S and S' are generators of $\mathcal{Q}^+(7,q)$ belonging to the same system. Here, $\mathcal{D}$ consists of q^2+1 generators belonging to each hyperbolic quadric of the pencil $\mathcal{F}$ such that every element in $\mathcal{D}$ meets S and S' in a projective line. It follows that $\mathcal{D}_S = \{A \cap S \mid A \in \mathcal{D}\}$ and $\mathcal{D}_{S'} = \{A \cap S' \mid A \in \mathcal{D}\}$ are both Desarguesian line–spreads of S and S', respectively. In other words $\mathcal{D}_S = \{\phi(P) \mid P \in \Sigma\}$ and $\mathcal{D}_{S'} = \{\phi(P) \mid P \in \Sigma'\}$.

Lemma 4.1. *There exists a group H in the orthogonal group* $\mathrm{PGO}^+(8,q)$*, stabilizing $\mathcal{Q}^+(7,q)$, fixing both S, S', their line–spreads $\mathcal{D}(S)$, $\mathcal{D}(S')$ and permuting in a single orbit the remaining lines of S (respectively S').*

Proof. Let r' be a line of S'. Then, $r'^{\perp}$ meets S in a line r. If r' belongs to $\mathcal{D}_{S'}$, then r belongs to $\mathcal{D}_S$. Assume that r' does not belong to $\mathcal{D}_{S'}$. Of course, r' meets $q+1$ lines $l'_1, \ldots, l'_{q+1}$ of $\mathcal{D}_{S'}$ and r meets $q+1$ lines $l_1, \ldots, l_{q+1}$ of $\mathcal{D}_S$. The subgroup of the orthogonal group $\mathrm{PGO}^+(8,q)$ fixing $\mathcal{Q}^+(7,q)$ and stabilizing both S and S' (but that does not interchange them) is isomorphic to $\mathrm{PGL}(4,q)$ (which in turn is isomorphic to a subgroup of index two of $\mathrm{PGO}^+(6,q)$). Under the Klein correspondence between lines of S and points of the Klein quadric $\mathcal{K} = \mathcal{Q}^+(5,q)$, the lines of $\mathcal{D}_S$ are mapped to a 3–dimensional elliptic quadric $\mathcal{E}$ embedded in $\mathcal{K}$ and the lines $l_1, \ldots, l_{q+1}$ are mapped to a conic section $\mathcal{C}$ of $\mathcal{E}$, see [13]. Also, there exists a subgroup H' of the orthogonal group $\mathrm{PGO}^+(6,q)$ fixing $\mathcal{K}$, having order $(q+1)|\mathrm{PGL}(2,q^2)|$, stabilizing $\mathcal{E}$ and permuting in a single orbit the remaining points of $\mathcal{K}$, see also [6, Proposition 3]. It follows that there exists a group H in the orthogonal group $\mathrm{PGO}^+(8,q)$ corresponding to H', stabilizing $\mathcal{Q}^+(7,q)$, fixing both S, S', their line–spreads $\mathcal{D}(S)$, $\mathcal{D}(S')$ and permuting in a single orbit the remaining lines of S (respectively S'), as required. $\square$

In the setting described in the proof of the previous Lemma, the line r corresponds, under the Klein correspondence, to a point P contained in the conic $\mathcal{C}' := \langle \mathcal{C} \rangle^{\perp_{\mathcal{K}}} \cap \mathcal{K}$ (here $\perp_{\mathcal{K}}$ denotes the orthogonal polarity of $\mathrm{PG}(5,q)$ induced by $\mathcal{K}$). The stabilizer of $\mathcal{C}$ in H' contains a subgroup, say H'', isomorphic to $\mathrm{PGL}(2,q)$. Every projectivity of H'' acts identically on the plane $\langle \mathcal{C} \rangle^{\perp_{\mathcal{K}}}$. Hence H'' fixes pointwise each of the $q(q-1)/2$ external lines E to the conic $\mathcal{C}'$ lying in the plane $\langle \mathcal{C} \rangle^{\perp_{\mathcal{K}}}$. Moreover, the group H'' has $q(q-1)/2$ orbits of size q^2-q. Each of them, together with $\mathcal{C}$, is the elliptic quadric $l^{\perp_{\mathcal{K}}} \cap \mathcal{K}$, for some $l \in E$. Also, these are all the elliptic quadrics of $\mathcal{K}$ on $\mathcal{C}$. Let $\mathcal{E}'$ be one of the above orbits of $H'_{\mathcal{C}}$ of size q^2-q disjoint from $\mathcal{E}$. Let $L_{\mathcal{E}'}$ be the set of lines of S corresponding to $\mathcal{E}'$. Let Y denote the solid generated by r' and a line of $L_{\mathcal{E}'}$.

Lemma 4.2. *Y^H is a set of q^6-q^2 solids mutually intersecting in at most a line.*

Proof. Consider the orbit Y^H of Y under the action of the group H. Since the lines in $L_{\mathcal{E}'}$ are mutually disjoint, then two distinct solids in Y^H containing r' have in common exactly the line r'. Let l be a line of $L_{\mathcal{E}'}$. Under the Klein correspondence, the line l corresponds to a point $P' \in \mathcal{E}'$. Notice that $P'^{\perp_{\mathcal{K}}}$ meets $\mathcal{E}$ in a conic, say $\mathcal{C}''$, that is necessarily disjoint from $\mathcal{C}$. Assume on the contrary that there exists a point in common between $\mathcal{C}$ and $\mathcal{C}''$, say Q. Then the line $P'Q$ is entirely contained in $\mathcal{K}$. Also, $P'Q \subset \mathcal{E}' = \langle P', \mathcal{C}'' \rangle \cap \mathcal{K}$, contradicting the fact that $\mathcal{E}'$ is a 3–dimensional elliptic quadric (and so does not contain lines). Now, we claim that the solid $\langle P, \mathcal{C}'' \rangle$ meets $\mathcal{K}$ in a 3–dimensional elliptic quadric. Indeed, otherwise, there would be a line entirely contained in $\mathcal{K}$ and passing through P. But such a line would contain a point of $\mathcal{C}''$, that clearly is a contradiction, since $P \in \mathcal{C}^{\perp_{\mathcal{K}}}$ and $\mathcal{C}''$ is disjoint from $\mathcal{C}$. It follows that if H_l denotes the stabilizer of l in H, then r^{H_l} contain q^2-q mutually disjoint lines. Therefore r'^{H_l} contain q^2-q mutually disjoint lines and two solids in Y^H containing l have in common exactly the line l. Then Y^H is a set of solids mutually intersecting in at most a line. Finally, the set Y^H contains $(q^2-q)(q^2+q)(q^2+1) = q^6-q^2$ solids. $\square$

We are ready to prove the main theorem of this Section.

Theorem 4.3. *There exists an* $(8, M, 4; 4)_q$ *constant–dimension subspace code, where*

$$M = q^{12} + q^2(q^2 + 1)^2(q^2 + q + 1) + 1.$$

Proof. Notice that none of the solids in Y^H is a generator of $\mathcal{Q}^+(7, q)$ or of a quadric of the pencil $\mathcal{F}$. Finally, assume that a solid T in Y^H generated by a line $l \in S$ and a line $r \in S'$ contains a plane π that is entirely contained in $\mathcal{Q}^+(7, q)$ or in a quadric of the pencil $\mathcal{F}$. Then, π would meet l' in a point U and hence T would meet S' in a line through U that is not the case. □

Corollary 4.4.

$$\mathcal{A}_q(8, 4; 4) \geq q^{12} + q^2(q^2 + 1)^2(q^2 + q + 1) + 1.$$

Remark 4.5. The result of Theorem 4.3 was obtained with different techniques in [7], where the authors, among other interesting results, proved that $q^{12} + q^2(q^2 + 1)^2(q^2 + q + 1) + 1$ is also the maximum size of an $(8, M, 4; 4)_q$ constant–dimension subspace code containing a lifted MRD code.

Acknowledgments. This work has been published in *Combinatorica* (2017). DOI 10.1007/s00493-016-3354-5.

References

[1] A. Beutelspacher, Partial spreads in finite projective spaces and partial designs, *Math. Z.* 145 (1975), no. 3, 211-229.

[2] J. M. N. Brown, Partitioning the complement of a simplex in $\mathrm{PG}(e, q^{d+1})$ into copies of $\mathrm{PG}(d, q)$, *J. Geom.* 33 (1988), no. 1-2. 11-16.

[3] A. Cossidente, F. Pavese, On subspace codes, *Des. Codes Cryptogr.* DOI 10.1007/s10623-014-0018-6.

[4] A. Cossidente, G. Marino, F. Pavese, Non–linear maximum rank distance codes, *Des. Codes Cryptogr.* DOI 10.1007/s10623-015-0108-0.

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

[6] R. H. Dye, Spreads and classes of maximal subgroups of $\mathrm{GL}(n, q)$, $\mathrm{SL}(n, q)$, $\mathrm{PGL}(n, q)$ and $\mathrm{PSL}(n, q)$, *Ann. Mat. Pura Appl.* (4) 158 (1991), 33-50.

[7] T. Etzion, N. Silberstein, Codes and Designs Related to Lifted MRD Codes, *IEEE Trans. Inform. Theory* 59 (2013), no. 2, 1004-1017.

[8] T. Etzion, N. Silberstein, Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams, *IEEE Trans. Inform. Theory* 55 (2009), no. 7, 2909-2919.

[9] T. Etzion, A. Vardy, Error-correcting codes in projective space, *IEEE Trans. Inform. Theory* 57 (2011), no. 2, 1165-1173.

[10] E. M. Gabidulin, Theory of codes with maximum rank distance, *Problems of Information Transmission* 21 (1985), 1-12.

[11] M. Gadouleau, Z. Yan, Constant-rank codes and their connection to constant-dimension codes, *IEEE Trans. Inform. Theory* 56 (2010), no. 7, 3207-3216.

[12] N. Gill, Polar spaces and embeddings of classical groups, *New Zealand J. Math.* 36 (2007), 175-184.

[13] J. W. P. Hirschfeld, *Finite projective spaces of three dimensions*, Oxford Mathematical Monographs, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1985.

[14] J. W. P. Hirschfeld, J. A. Thas, *General Galois Geometries*, Oxford Mathematical Monographs, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1991.

[15] T. Honold, M. Kiermaier, S. Kurz, Optimal binary subspace codes of length 6, constant dimension 3 and minimum distance 4, Topics in finite fields, 157-176, *Contemp. Math.*, 632, Amer. Math. Soc., Providence, RI, 2015.

[16] B. Huppert, *Endliche Gruppen I*, Die Grundlehren der Mathematischen Wissenschaften, Springer-Verlag, Berlin-New York, 1967.

[17] A. Khaleghi, D. Silva, F. R. Kschischang, Subspace codes, *Cryptography and coding*, 1-21, Lecture Notes in Comput. Sci., Springer, Berlin, 2009.

[18] P. Kleidman, M. Liebeck, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Note Series, vol. 129 Cambridge University Press, Cambridge, 1990.

[19] A. Klein, K. Metsch, L. Storme, Small maximal partial spreads in classical finite polar spaces, *Adv. Geom.* 10 (2010), no. 3, 379-402.

[20] R. Koetter, F. R. Kschischang, Coding for errors and erasures in random network coding, *IEEE Trans. Inform. Theory*, 54 (8), 3579-3591, Aug. 2008.

[21] M. Lavrauw, G. Van de Voorde, Field reduction and linear sets in finite geometry, Topics in finite fields, 271-293, *Contemp. Math.*, 632, Amer. Math. Soc., Providence, RI, 2015.

[22] G. Lunardon, G. Marino, O. Polverino, R. Trombetti, Maximum scattered linear sets of pseudoregulus type and the Segre Variety $\mathcal{S}_{n,n}$, *J. Algebr. Comb.*, 39 (2014), 807-831.

[23] R. M. Roth, Maximum-rank array codes and their application to crisscross error correction, *IEEE Trans. Inform. Theory*, 37 (1991), 328-336.

[24] B. Segre, Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane, *Ann. Mat. Pura Appl.* 64 (1964), 1-76.

[25] D. Silva, F. R. Kschischang, R. Koetter, A rank-metric approach to error control in random network coding, *IEEE Trans. Inform. Theory*, vol. 54, pp. 3951-3967, September 2008.

[26] A.-L. Trautmann, J. Rosenthal, New improvements on the echelon-Ferrers construction, in proc. of *Int. Symp. on Math. Theory of Networks and Systems*, 405-408, July 2010.

[27] S.-T. Xia, F.-W. Fu, Johnson type bounds on constant dimension codes, *Des. Codes Cryptogr.*, (50) 2009, 163-172.