Discrete Applied Mathematics 186 (2015) 87–97

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

Equidistant codes in the Grassmannian

Tuvi Etzion *, Netanel Raviv

Department of Computer Science, Technion, Haifa 32000, Israel

ARTICLE INFO

Article history:
Received 13 October 2013
Received in revised form 24 December 2014
Accepted 13 January 2015
Available online 12 February 2015

Keywords:
Constant rank codes
Equidistant codes
Grassmannian
Plücker embedding
Sunflower

ABSTRACT

Equidistant codes over vector spaces are considered. For k-dimensional subspaces over a large vector space the largest code is always a sunflower. We present several simple constructions for such codes which might produce the largest non-sunflower codes. A novel construction, based on the Plücker embedding, for 1-intersecting codes of k-dimensional subspaces over $\mathbb{F}_q^n$, $n \geq \binom{k+1}{2}$, where the code size is $\frac{q^{k+1}-1}{q-1}$ is presented. Finally, we present a related construction which generates equidistant constant rank codes with matrices of size $n \times \binom{n}{2}$ over $\mathbb{F}_q$, rank $n-1$, and rank distance $n-1$.

1. Introduction

Equidistant codes in the Hamming scheme are the bridge between coding theory and extremal combinatorics. A code is called equidistant if the distance between any two distinct codewords is equal to a given parameter d. A code which is represented as a collection of subsets will be called *t-intersecting* if the intersection between any two codewords is exactly t. A binary code of length n in the Hamming scheme is a collection of binary words of length n. A binary code of length n with m codewords can be represented as a binary $m \times n$ matrix whose rows are the codewords of the code. The Hamming distance between two codewords is the number of positions in which they differ. The *weight* of a word is the number of nonzero entries in the word. A code **C** is called *a constant weight code* if all its codewords have the same weight. The *minimum Hamming distance* of the code is the smallest distance between two distinct codewords. An (n, d, w) code is a constant weight code of length n, weight w, and minimum Hamming distance d. Optimal t-intersecting equidistant codes (which must be also constant weight) have two very interesting families of codes, codes obtained from projective planes and codes obtained from Hadamard matrices [6].

Recently, there have been lot of new interest in codes whose codewords are vector subspaces of a given vector space over $\mathbb{F}_q$, where $\mathbb{F}_q$ is the finite field with q elements. The interest in these codes is a consequence of their application in random network coding [24]. These codes are related to what are known as q-analogs. The well known concept of q-analogs replaces subsets by subspaces of a vector space over a finite field and their sizes by the dimensions of the related subspaces. A binary codeword can be represented by a subset whose elements are the nonzero positions. In this respect, *constant dimension codes* are the q-analog of constant weight codes. For a positive integer n, the set of all subspaces of $\mathbb{F}_q^n$ is called the *projective space* $\mathcal{P}_q(n)$. The set of all k-dimensional subspaces (k-subspaces in short) of $\mathbb{F}_q^n$ is called a *Grassmannian* and is denoted by $\mathcal{G}_q(n,k)$. The size of $\mathcal{G}_q(n,k)$ is given by the q-binomial coefficient $\begin{bmatrix} n \\ k \end{bmatrix}_q$, i.e.

$$|\mathcal{G}_q(n,k)| = \begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}.$$

* Corresponding author.
E-mail addresses: etzion@cs.technion.ac.il (T. Etzion), netanel.raviv@gmail.com (N. Raviv).

http://dx.doi.org/10.1016/j.dam.2015.01.024

Similarly, the set of all k-subspaces of a subspace V is denoted by $\begin{bmatrix} V \\ k \end{bmatrix}_q$. It turns out that the natural measure of distance in $\mathcal{P}_q(n)$ is given by

$$d_S(X, Y) = \dim X + \dim Y - 2\dim\big(X \cap Y\big),$$

for all $X, Y \in \mathcal{P}_q(n)$. This measure of distance is called the *subspace distance* and it is the q-analog of the Hamming distance in the Hamming space. Finally, an $[n, d, k]_q$ code is a subset of $\mathcal{G}_q(n, k)$ (constant dimension code), having minimum subspace distance d, where the minimum subspace distance of the code is the smallest subspace distance between any two codewords. In the sequel, when distance will be mentioned it will be understood from the context if the Hamming distance or the subspace distance is used.

The main goal of this paper is to consider the t-intersecting constant dimension codes (which are clearly equidistant). In this context interesting constructions of such codes were given in [19,20], but their size is rather small.

Some optimal binary equidistant codes form a known structure from extremal combinatorics called a partial projective plane. This structure was defined and studied in [17]. An important concept in this context is the sunflower. A binary constant weight code of weight w is called a *sunflower* if any two codewords intersect in the same t coordinates. A *sunflower* $\mathbb{S} \subset \mathcal{G}_q(n, k)$ is a t-intersecting equidistant code in which any two codewords $X, Y \in \mathbb{S}$ intersect in the same t-subspace Z. The t-subspace Z is called the *center* of $\mathbb{S}$ and is denoted by $Cen(\mathbb{S})$.

An upper bound on the size of t-intersecting binary constant weight code with weight w was given in [6,7]. If the size of such code is greater than $(w-t)^2 + (w-t) + 1$ then the code is a sunflower. This bound is attained when $t = 1, w = q+1$, where q is a prime power and the codewords are the characteristic vectors of length $\begin{bmatrix} n \\ 1 \end{bmatrix}_q$ which represent the lines of the projective plane of order q. Except for some specific cases [18] no better bound is known. This bound can be adapted for t-intersecting constant dimension codes with dimension k over $\mathbb{F}_q$. We can view the characteristic binary vectors with weight $\frac{q^k-1}{q-1}$ as the codewords, which implies intersection of size $\frac{q^t-1}{q-1}$ between codewords and hence we have the following bound.

Theorem 1. *If a t-intersecting constant dimension code of dimension k has more than $\left(\frac{q^k-q^t}{q-1}\right)^2 + \frac{q^k-q^t}{q-1} + 1$ codewords, then the code is a sunflower.*

The bound of Theorem 1 is rather weak compared to the known lower bounds. The following conjecture [4] is attributed to Deza.

Conjecture 1. *If a t-intersecting code in $\mathcal{G}_q(n, k)$ has more than $\begin{bmatrix} k+1 \\ 1 \end{bmatrix}_q$ codewords, then the code is a sunflower.*

The term t-intersecting code is different from the highly related term t-intersecting family [10,13]. A family of k-subsets of a set X is called t-intersecting if any two k-subsets in the family intersect in at least t elements [10]. The celebrated Erdös–Ko–Rado theorem determines the maximum size of such family. The q-analog problem was considered for subspaces in [23,13]. For the q-analog problem, a t-intersecting family is a set of k-subspaces whose pairwise intersection is at least t. In [13] it was proved that

Theorem 2. *If $\mathbb{I} \subseteq \mathcal{G}_q(n, k)$ is a family of k-subspaces of $\mathbb{F}_q^n$ whose pairwise intersection is of dimension at least t, then*

$$|\mathbb{I}| \le \max\left\{ \begin{bmatrix} n-t \\ k-t \end{bmatrix}_q, \begin{bmatrix} 2k-t \\ k \end{bmatrix}_q \right\}.$$

Although Theorem 2 concerns fundamentally different families from the ones discussed in this paper, some intriguing resemblance is evident. One can easily see that there exist two simple families of subspaces attaining the bound of Theorem 2. The first is the set of all k-subspaces sharing at least a fixed t-subspace. The second is the set of all k-subspaces contained in some $(2k-t)$-subspace. These elements are closely related to the terms *sunflower* and *ball* discussed in detail in Section 2.

One concept which is heavily connected to constant dimension codes is rank-metric codes. For two $k \times \ell$ matrices A and B over $\mathbb{F}_q$ the *rank distance* is defined by

$$d_R(A, B) = \text{rank}(A - B).$$

A $[k \times \ell, \varrho, \delta]$ *rank-metric code* $\mathcal{C}$ is a linear code, whose codewords are $k \times \ell$ matrices over $\mathbb{F}_q$; they form a linear subspace with dimension ϱ of $\mathbb{F}_q^{k\times\ell}$, and for each two distinct codewords A and B we have that $d_R(A, B) \ge \delta$.

There is a large literature on rank-metric code and also on the connections between rank-metric codes and constant dimension codes, e.g. [5,11,15,16,28,29]. Given a rank-metric code, one can form from it a constant dimension code, by lifting its matrices [11,29]. Optimal constant dimension codes can be derived from optimal codes of a subclass of rank-metric codes, namely *constant rank codes*. In a constant rank code all matrices have the same rank. The connection between optimal codes in this class and optimal constant dimension codes was given in [16]. This also can motivate a research on equidistant constant rank codes which we will also discuss in this paper.

The rest of this paper is organized as follows. In Section 2 we consider trivial codes and trivial constructions. The trivial equidistant constant dimension codes are the q-analogs of the trivial binary equidistant constant weight codes. It will be very clear that the trivial q-analogs are not so trivial. In fact for most parameters we do not know the size of the largest trivial codes. We will also define two operations which are important in constructions of codes. The first one is the extension of a code (or the extended code of a given code) preserves the triviality of the code. The second operation is the orthogonality (or the orthogonal code of a given code) preserves triviality only in one important set of parameters. In Section 3 we present our main result of the paper, a construction of 1-intersecting code in $\mathcal{G}_q(n, k)$, $n \geq \binom{k+1}{2}$, whose size is $\begin{bmatrix} k+1 \\ 1 \end{bmatrix}_q$. The construction is based on the Plücker embedding [2]. We will show one case in which a larger code by one is obtained, which falsifies Conjecture 1 in this case. We also consider the largest non-sunflower t-intersecting codes in $\mathcal{G}_q(n, k)$ based on our discussion. Finally, we consider the size of the largest equidistant code in all the projective space $\mathcal{P}_q(n)$. In Section 4 we use the Plücker embedding to form a constant rank code over $\mathbb{F}_q$, with matrices of size $n \times \binom{n}{2}$, rank $n-1$, rank distance $n-1$, and $q^n - 1$ codewords. The technique of Section 4 is used in Section 5 for a recursive construction of exactly the same codes constructed in Section 3. Conclusion and open problems for future research are given in Section 6.

2. Trivial codes and trivial constructions

In this section we will consider first trivial codes. A binary constant weight equidistant code **C** of size m is called *trivial* if every column of **C** has m or $m-1$ equal entries. Now, we define a q-analog for a constant dimension equidistant code. A constant dimension equidistant code $\mathbb{C} \subset \mathcal{G}_q(n, k)$ will be called *trivial* if one of the following two conditions holds.

1. Each element x of $\mathbb{F}_q^n$ is either contained in all k-subspaces of $\mathbb{C}$, no k-subspace of $\mathbb{C}$, or exactly one k-subspace of $\mathbb{C}$.
2. If $\mathbb{T}$ is the smallest subspace of $\mathbb{F}_q^n$ which contains all the k-subspaces of $\mathbb{C}$ then $\mathbb{T}$ is a $(k+1)$-subspace.

A trivial code which satisfies the first condition is a *sunflower*. A trivial code which satisfies the second condition will be called a *ball*. We will examine now the types of constant dimension equidistant codes which satisfy one of these two conditions. We will discover that in some cases triviality does not mean that it is easy to find the optimal (largest) trivial code.

2.1. Partial spreads

Two subspaces $X, Y \in \mathcal{G}_q(n, k)$ are called *disjoint* if their intersection is the null space, i.e. $X \cap Y = \{\mathbf{0}\}$. A *partial k-spread* (or a *partial spread* in short) in $\mathcal{G}_q(n, k)$ is a set of disjoint subspaces from $\mathcal{G}_q(n, k)$. If k divides n and the partial spread has $\frac{q^n-1}{q^k-1}$ subspaces then the partial spread is called a *k-spread* (or a *spread* in short). A partial spread in $\mathcal{G}_q(n, k)$ is the q-analog of a 0-intersecting constant weight code of length n and weight k. The number of k-subspaces in the largest partial spread of $\mathcal{G}_q(n, k)$ will be denoted by $E_q[n, k]$. The known upper and lower bounds on $E_q[n, k]$ are summarized in the following theorems. The first three well-known theorems can be found in [12].

Theorem 3. *If k divides n then* $E_q[n, k] = \frac{q^n-1}{q^k-1}$.

Theorem 4. $E_q[n, k] \leq \left\lfloor \frac{q^n-1}{q^k-1} \right\rfloor - 1$ *if* $n \not\equiv 0 \pmod k$.

Theorem 5. *Let $n \equiv r \pmod k$. Then, for all q, we have*

$$E_q[n, k] \geq \frac{q^n - q^k(q^r - 1) - 1}{q^k - 1}.$$

The next theorem was proved in [22] for $q = 2$ and for any other q in [1].

Theorem 6. *If $n \equiv 1 \pmod k$ then* $E_q[n, k] = \frac{q^n-q}{q^k-1} - q + 1 = \sum_{i=1}^{\frac{n-1}{k}-1} q^{ik+1} + 1$.

Theorem 6 was extended for the case where $q = 2$ and $k = 3$ in [9] as follows.

Theorem 7. *If $n \equiv c \pmod 3$ then* $E_2[n, 3] = \frac{2^n-2^c}{7} - c$.

The upper bound implied by Theorem 6 was improved for some cases in [8].

Theorem 8. *If $n = k\ell + c$ with $0 < c < k$, then* $E_q[n, k] \leq \sum_{i=0}^{\ell-1} q^{ik+c} - \Omega - 1$, *where* $2\Omega = \sqrt{1 + 4q^k(q^k - q^c)} - (2q^k - 2q^c + 1)$.

2.2. Extension of a code

An (n, d, w) constant weight equidistant code **C** is *extended* to an $(n+1, d, w+1)$ constant weight equidistant code $\mathcal{E}(\mathbf{C})$ by adding a column of *ones* to the code. Similarly, an $[n, d, k]_q$ constant dimension equidistant code $\mathbb{C}$ is *extended* to an $[n+1, d, k+1]_q$ constant dimension equidistant code $\mathcal{E}(\mathbb{C})$ as follows. We first define $\mathbb{F}_q^{n+1}$ by $\mathbb{F}_q^{n+1} = \{(x, \alpha) \mid x \in \mathbb{F}_q^n,\ \alpha \in \mathbb{F}_q\}$. For a subspace $X \in \mathcal{G}_q(n, k)$ let $(X, 0)$ be a subspace in $\mathcal{G}_q(n+1, k)$ defined by $(X, 0) = \{(x, 0) \mid x \in X\}$. Let $v \in \mathbb{F}_q^{n+1} \setminus \{(x, 0) \mid x \in \mathbb{F}_q^n\}$ and $\mathbb{C} \subset \mathcal{G}_q(n, k)$. We define the extended code $\mathcal{E}(\mathbb{C})$ by

$$\mathcal{E}(\mathbb{C}) = \{\langle (X, 0) \cup \{v\} \rangle \mid X \in \mathbb{C}\}.$$

The following theorem can be easily verified.

Theorem 9. *If* $\mathbf{C}$ *and* $\mathbb{C}$ *are trivial codes, then the extended codes* $\mathcal{E}(\mathbf{C})$ *and* $\mathcal{E}(\mathbb{C})$ *are also trivial codes.*

We note that the extended code $\mathcal{E}(\mathbb{C})$ of a trivial code $\mathbb{C}$ is not unique, but all such extended codes are isomorphic. An $[n, d, k]_q$ constant dimension equidistant code $\mathbb{C}$ can be extended ℓ times to an $[n+\ell, d, k+\ell]_q$ constant dimension equidistant code. This extended code will be denoted by $\mathcal{E}^{\ell}(\mathbb{C})$.

2.3. Sunflowers

A partial spread is clearly a 0-intersecting sunflower. For a given n, k such that $0 < k < n$ we construct the largest t-intersecting sunflower in $\mathcal{G}_q(n, k)$ by using the following two simple theorems.

Theorem 10. *If* $\mathbb{S}$ *is a* t*-intersecting sunflower in* $\mathcal{G}_q(n, k)$*, then* $\mathcal{E}(\mathbb{S})$ *is a* $(t+1)$*-intersecting sunflower in* $\mathcal{G}_q(n+1, k+1)$.

Theorem 11. *Let* $\mathbb{S}$ *be a* t*-intersecting sunflower in* $\mathcal{G}_q(n, k)$ *and let* X *be an* $(n-t)$*-subspace of* $\mathbb{F}_q^n$ *such that* $X \oplus Cen(\mathbb{S}) = \mathbb{F}_q^n$*. Then the set* $\{X \cap Y \mid Y \in \mathbb{S}\}$ *is a partial* $(k-t)$*-spread in* X.

If $\mathbb{S}$ is the largest partial $(k-t)$-spread in $\mathcal{G}_q(n-t, k-t)$, then by Theorem 10 we have that $\mathcal{E}^t(\mathbb{S})$ is a t-intersecting sunflower in $\mathcal{G}_q(n, k)$. By Theorem 11, we have that $\mathcal{E}^t(\mathbb{S})$ is the largest t-intersecting sunflower in $\mathcal{G}_q(n, k)$.

2.4. Optimal $(k-1)$-intersecting equidistant codes in $\mathcal{G}_q(n, k)$

In this subsection we present a construction for optimal $(k-1)$-intersecting equidistant code in $\mathcal{G}_q(n, k)$ for any $n \geq k+1$.

Theorem 12. *An optimal non-sunflower* $(k-1)$*-intersecting equidistant code in* $\mathcal{G}_q(n, k)$*,* $n \geq k+1$ *has* $\begin{bmatrix} k+1 \\ k \end{bmatrix}_q$ *subspaces.*

Proof. Let V be any $(k+1)$-subspace of $\mathbb{F}_q^n$ and let $\mathbb{C} = \begin{bmatrix} V \\ k \end{bmatrix}_q$, i.e. $\mathbb{C}$ consists of all k-subspaces of a $(k+1)$-subspace. It is readily verified that every two such k-subspaces intersect at a $(k-1)$-subspace, and the size of $\mathbb{C}$ is $\begin{bmatrix} k+1 \\ k \end{bmatrix}_q$.

Let $\mathbb{C}'$ be an equidistant $(k-1)$-intersecting code in $\mathcal{G}_q(n, k)$. Let $X \in \mathbb{C}'$, and let $\mathbb{S}_1, \mathbb{S}_2$ be any two distinct sunflowers in $\mathbb{C}'$ such that $Cen(\mathbb{S}_1), Cen(\mathbb{S}_2) \subseteq X$. It is easy to verify that for every $X_1 \in \mathbb{S}_1, X_2 \in \mathbb{S}_2$ (which implies that $\dim(X_1 \cap X_2) = k-1$) we have that $|X_1 \cap X_2 \cap X| = q^{k-2} - 1$ which implies that $|X_1 \cap X_2 \cap X^c| = (q^{k-1} - 1) - (q^{k-2} - 1) = (q-1)q^{k-2}$.

We prove now that for every $X_1 \in \mathbb{S}_1$ and every $Y, Z \in \mathbb{S}_2$ the sets $\mathcal{A} = X_1 \cap Y \cap X^c$ and $\mathcal{B} = X_1 \cap Z \cap X^c$ are mutually disjoint. Since $Y, Z \in \mathbb{S}_2$ and $Cen(\mathbb{S}_2) \subseteq X$, it follows that Y and Z do not intersect outside X, i.e. $(Y \cap Z) \cap X^c = \varnothing$. If $\mathcal{A} \cap \mathcal{B} \neq \varnothing$ or equivalently $X_1 \cap Y \cap Z \cap X^c \neq \varnothing$ then $Y \cap Z \cap X^c \neq \varnothing$, a contradiction.

Therefore, in the set $\{X_1 \cap Y \cap X^c \mid Y \in \mathbb{S}_2\}$ there can be at most $(q^k - q^{k-1})/(q-1)q^{k-2} = q$ disjoint subsets of size $(q-1)q^{k-2}$. Hence, the size of any sunflower other than $\mathbb{S}_1$ is at most $q+1$. However, all of the above arguments are applicable for any initial sunflower $\mathbb{S}_1$. Therefore, each sunflower whose center is inside X have at most $q+1$ codewords, including X itself. X may have at most $\begin{bmatrix} k \\ k-1 \end{bmatrix}_q$ sunflower centers inside it, which yields that:

$$|\mathbb{C}'| \leq 1 + q \cdot \begin{bmatrix} k \\ k-1 \end{bmatrix}_q = \begin{bmatrix} k+1 \\ k \end{bmatrix}_q = |\mathbb{C}|.$$

Thus, the claim in the theorem follows. □

Corollary 1. *An optimal non-sunflower equidistant* $(k-1)$*-intersecting code in* $\mathcal{G}_q(n, k)$*,* $n \geq k+1$ *consists of all* k*-subspaces of any given* $(k+1)$*-subspace. This code is a trivial code which satisfies the second condition, i.e., it is a ball.*

2.5. Orthogonal subspaces

A simple operation which preserves the equidistant property of a code and its triviality in the Hamming scheme is the *complement*. Two binary words $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ are *complements* if for each i, $1 \leq i \leq n$, we have $x_i + y_i = 1$, i.e., $x_i = 0$ if and only if $y_i = 1$. We say that y is the complement of x and denote it by $y = \bar{x}$. For a binary code $\mathbf{C}$, the *complement* of $\mathbf{C}$, $\bar{\mathbf{C}}$ is defined by $\bar{\mathbf{C}} = \{x \mid \bar{x} \in \mathbf{C}\}$. It is easily verified that if a constant weight code $\mathbf{C}$ is equidistant then also its complement is constant weight code and equidistant and if $\mathbf{C}$ is trivial then also its complement $\bar{\mathbf{C}}$ is trivial.

What is the q-analog operation for the complement? This question was discussed in detail before [3]. We will use the orthogonality as the q-analog for complement. For a constant dimension code $\mathbb{C} \subseteq \mathcal{G}_q(n, k)$ we define the *orthogonal* code by $\mathbb{C}^{\perp} = \{X \mid X^{\perp} \in \mathbb{C}\}$. It is known [12,24,30] that for any two subspaces $X, Y \in \mathbb{F}_q^n$ we have $d_S(X, Y) = d_S(X^{\perp}, Y^{\perp})$. This immediately implies the following result.

Theorem 13. *If $\mathbb{C}$ is a t-intersecting equidistant code in $\mathcal{G}_q(n,k)$, then $\mathbb{C}^{\perp}$ is a t'-intersecting equidistant code in $\mathcal{G}_q(n,n-k)$, where $t' = n-2k+t$.*

Proof. Clearly, $\mathbb{C}^{\perp}$ is a code in $\mathcal{G}_q(n, n-k)$. Furthermore, $\mathbb{C}$ and $\mathbb{C}^{\perp}$ have the same minimum subspace distance d which is also the distance between any two codewords of $\mathbb{C}$ and between any two codewords of $\mathbb{C}^{\perp}$. Therefore, $d = 2(k-t) = 2(n-k-t')$ which implies $t' = n-2k+t$. $\square$

Corollary 2. *If $\mathbb{C}$ is a 0-intersecting code in $\mathcal{G}_q(n,k)$ (a partial spread), then $\mathbb{C}^{\perp}$ is an $(n-2k)$-intersecting code in $\mathcal{G}_q(n,n-k)$.*

Corollary 3. *The smallest possible n for which a t-intersecting code exists in $\mathcal{G}_q(n,k)$ is $n = 2k-t$. The size of the largest such code is the size of the largest partial spread in $\mathcal{G}_q(2k-t, k-t)$.*

The next question we would like to answer is whether the orthogonal code of a trivial code is also a trivial code. The answer is that usually, the orthogonal code of a trivial code is not a trivial code. The only exception is given in the following theorem whose proof is easy to verify.

Theorem 14. *$\mathbb{C}$ is an optimal $(k-1)$-intersecting equidistant code in $\mathcal{G}_q(n,k)$ (a ball) if and only if $\mathbb{C}^{\perp}$ is a $(n-k-1)$-intersecting sunflower in $\mathcal{G}_q(n,n-k)$.*

3. Constructions of large non-sunflower equidistant codes

In this section, we will consider the size of the largest non-sunflower equidistant code in $\mathcal{G}_q(n,k)$ and in $\mathcal{P}_q(n)$. The main result which will be presented in Section 3.1 is a construction of 1-intersecting codes in $\mathcal{G}_q(n,k)$, $n \geq \binom{k+1}{2}$, whose size is $\begin{bmatrix} k+1 \\ 1 \end{bmatrix}_q$. This construction will be based on the Plücker embedding. In Section 3.2 we will show the only example we have found (by computer search) for which this construction is not optimal. In Section 3.3 we will consider the largest non-sunflower t-intersecting codes in $\mathcal{G}_q(n,k)$ based on our discussion. In Section 3.4 we will consider the size of the largest equidistant code in the whole projective space $\mathcal{P}_q(n)$.

3.1. Construction using the Plücker embedding

Let $[n]$ denote the set $\{1,2,\ldots,n\}$, let e_i denote the unit vector (of a given length) with a 1 in the ith coordinate, and for any $0 < k \leq n$, let $n_k = \binom{n}{k}$. We denote by $\mathbb{P}_q^{\ell-1}$ the set of *projective points* of $\mathbb{F}_q^{\ell}$. The set $\mathbb{P}_q^{\ell-1}$ is commonly referred to as the set $\mathbb{F}_q^{\ell}/\!\sim$ where $\sim$ is an equivalence relation over $\mathbb{F}_q^{\ell} \setminus \{0\}$ defined as

$$x \sim y \iff \exists \lambda \in \mathbb{F}_q \setminus \{0\}, x = \lambda y.$$

It is widely known [2,26,27] that $\mathcal{G}_q(n,k)$ can be embedded in $\mathbb{P}_q^{n_k-1}$ using the Plücker embedding, denoted by P.

Given $U \in \mathcal{G}_q(n,k)$, let $M(U) \in \mathbb{F}_q^{k\times n}$ be some $k \times n$ matrix over $\mathbb{F}_q$ whose row span is U. Given any k-subset $\{i_1,\ldots,i_k\}$ of $[n]$, let $M(U)(i_1,\ldots,i_k)$ be the $k\times k$ sub-matrix of $M(U)$ consisting of columns $i_1,\ldots,i_k$. Consider the $\binom{n}{k}$ coordinates of $\mathbb{F}_q^{n_k}$ as numbered by k-subsets of $[n]$, and for each k-subset $\{i_1,\ldots,i_k\}$ of $[n]$ assume w.l.o.g that $i_1 < \cdots < i_k$. The function P maps a subspace $U \in \mathcal{G}_q(n,k)$ to the equivalence class of the vector $v(U) \in \mathbb{F}_q^{n_k}$, defined as:

$$(v(U))_{\{i_1,\ldots,i_k\}} = \det M(U)(i_1,\ldots,i_k).$$

Namely, the coordinate $\{i_1,\ldots,i_k\}$ of the vector $v(U)$ is the determinant of the sub-matrix of $M(U)$ consisting of columns $i_1 < \cdots < i_k$ of $M(U)$. Formally, the function P is defined as $P(U) = [v(U)]$, where $[v(U)]$ is the equivalence class of the vector $v(U)$ under the equivalence relation $\sim$ defined earlier in this section. It is worth mentioning that the function P is well-defined, as any choice of a matrix $M(U)$ whose row span is U will result in the same equivalence class in $\mathbb{P}_q^{n_k-1}$ [2]. In this paper, in order to maintain consistency with coding theory terminology, we identify the set $\mathbb{P}_q^{\ell-1}$ by the set of all 1-subspaces of $\mathbb{F}_q^{\ell}$, namely, $\mathcal{G}_q(\ell,1)$.

Another concept we use in this section is Steiner systems. A *Steiner system* $S(t,k,n)$ is a pair (Q,B) where Q is an n-set of elements (called *points*) and B is a collection of k-subsets of Q (called *blocks*), such that every t-subset of Q is contained in exactly one block of B. A Steiner system can be described by its incidence matrix. This is a matrix $A = (a_{ij})$, $i \in [n]$, $j \in [b]$, $b = |S(t,k,n)|$, where if $Q = \{q_1,\ldots,q_n\}$ and $B = \{B_1,\ldots,B_b\}$ we have:

$$a_{ij} = \begin{cases} 1 & \text{if } q_i \in B_j \\ 0 & \text{if } q_i \notin B_j \end{cases}.$$

The following lemma, which is a key in the construction which follows, can be easily verified.

Lemma 1. *The rows of the matrix A defined by a Steiner system $S(2,k,n)$ form an 1-intersecting equidistance code. The weight of each codeword in this code is $\frac{n-1}{k-1}$.*

In what follows, we use the Plücker embedding, together with Lemma 1 to construct equidistant constant dimension codes.

Theorem 15. *For every integer $n \geq 3$, there exists an 1-intersecting equidistant code in $\mathcal{G}_q(n_2, n-1)$ of size $\begin{bmatrix} n \\ 1 \end{bmatrix}_q$, where $n_2 = \binom{n}{2}$.*

The main idea of the construction in the proof of Theorem 15 is to consider a set (design) $\mathcal{S}_{q,n}$ of blocks, whose blocks are the elements of $\mathcal{G}_q(n, 2)$ and its set of points is $\mathcal{G}_q(n, 1)$ where a point $X \in \mathcal{G}_q(n, 1)$ is incident with a block $Y \in \mathcal{G}_q(n, 2)$ if $X \subseteq Y$. $\mathcal{S}_{q,n}$ forms a Steiner system $S(2, q+1, \frac{q^n-1}{q-1})$ since every 2-subspace contains $q+1$ points and every pair of distinct 1-subspaces is contained in a unique 2-subspace. We embed $\mathcal{G}_q(n, 2)$ into $\mathbb{P}_q^{n_2-1}$ using the Plücker embedding, and show that given $V \in \mathcal{G}_q(n, 1)$, the set

$$P_V = \bigcup_{\substack{U \in \mathcal{G}_q(n,2) \\ V \subseteq U}} P(U)$$

is the union of the Plücker embeddings of subspaces in $\mathcal{G}_q(n, 2)$ which intersect at V and constitutes a subspace in $\mathcal{G}_q(n_2, n-1)$. Therefore, we may use Lemma 1 to get an 1-intersecting equidistant code in $\mathcal{G}_q(n_2, n-1)$ of size $\begin{bmatrix} n \\ 1 \end{bmatrix}_q = \frac{q^n-1}{q-1}$. The proof of Theorem 15 relies on the following two lemmas.

Lemma 2. $|P_V| = q^{n-1}$.

Proof. Note that the number of 2-subspaces that contain a given 1-subspace is $\frac{q^{n-1}-1}{q-1}$. Since each two distinct 1-subspaces $P(U_1), P(U_2)$ intersect trivially, it follows that $|P_V| = \frac{q^{n-1}-1}{q-1} \cdot (q-1) + 1 = q^{n-1}$. □

Lemma 3. *If $V \in \mathcal{G}_q(n, 1)$ then $P_V \in \mathcal{G}_q(n_2, n-1)$.*

Proof. Let v be an arbitrary nonzero vector in V. Let r be an arbitrary index such that $v_r \neq 0$ and let $\mathcal{B}_v = \{z^1, \ldots, z^{n-1}\}$ be the set of $n-1$ distinct unit vectors of length n such that $e_r \notin \mathcal{B}_v$. If $Z_i = \langle \{v, z^i\} \rangle$, $1 \leq i \leq n-1$, then by the definition of Plücker embedding, the projective point $P(Z_i)$, considered as an 1-subspace of $\mathbb{F}_q^{n_2}$, is the span of the vector p^i of length n_2, whose coordinates are indexed by the subsets $\{s, t\} \subseteq [n]$ and are defined by

$$p^i_{\{s,t\}} = \det_{(s,t)} \begin{pmatrix} v \\ z^i \end{pmatrix} = v_s z^i_t - v_t z^i_s. \tag{1}$$

Recall that the coordinates of $\mathbb{F}_q^{n_2}$ are identified with 2-subsets of $[n]$ as mentioned earlier in this section.

We will now prove that $\langle \{p^1, \ldots, p^{n-1}\} \rangle = P_V$, and since $|P_V| = q^{n-1}$ by Lemma 2, it implies that P_V is an $(n-1)$-subspace of $\mathbb{F}_q^{n_2}$.

Let $x = \sum_{i \in [n-1]} a_i p^i$ where $a_i \in \mathbb{F}_q$ for all $i \in [n-1]$. We will show that $x \in P_V$, i.e. that there exists a $\tilde{Z} \in \mathcal{G}_q(n_2, 2)$ such that $V \subseteq \tilde{Z}$ and $x \in P(\tilde{Z})$. As a consequence, we will have that $\langle \{p^1, \ldots, p^{n-1}\} \rangle \subseteq P_V$. Let

$$\tilde{z} = \sum_{i \in [n-1]} a_i z^i. \tag{2}$$

Clearly, $V \subseteq \langle \{v, \tilde{z}\} \rangle$, and since $\tilde{z}_r = 0$, $v_r \neq 0$ it follows that $\langle \{v, \tilde{z}\} \rangle$ is a 2-subspace of $\mathbb{F}_q^n$. By the definition of the Plücker embedding, $P\left(\langle \{v, \tilde{z}\} \rangle\right)$ is the span of the vector $\tilde{x}$, whose coordinates are indexed by the subsets $\{s, t\} \subseteq [n]$ and are defined by

$$\begin{aligned}
\tilde{x}_{\{s,t\}} &= \det_{(s,t)} \begin{pmatrix} v \\ \tilde{z} \end{pmatrix} \\
&= v_s \tilde{z}_t - v_t \tilde{z}_s \\
&= v_s \left(\sum_{i \in [n-1]} a_i z^i_t \right) - v_t \left(\sum_{i \in [n-1]} a_i z^i_s \right) \quad \text{by (2)} \\
&= \sum_{i \in [n-1]} a_i \left(v_s z^i_t - v_t z^i_s \right) \\
&= \sum_{i \in [n-1]} a_i p^i_{\{s,t\}} \quad \text{by (1)} \\
&= x_{\{s,t\}} \quad \text{by the definition of } x.
\end{aligned}$$

Hence $\tilde{x} = x$ and therefore $\langle \{p^1, \ldots, p^{n-1}\} \rangle \subseteq P_V$.

Now, let $x \in P_V$ and let $U_x \in \mathcal{G}_q(n, 2)$ be the unique 2-subspace such that $V \subseteq U_x$ and $x \in P(U_x)$. Hence, $U_x = \langle\{v, z\}\rangle$ for some $z \in \mathbb{F}_q^n$. By the definition of $\mathcal{B}_v = \{z^1, \dots, z^{n-1}\}$ every vector whose rth entry is 0 is in $\langle \mathcal{B}_v \rangle$. If $z_r \neq 0$ then we define

$$z' = v - \left(\frac{v_r}{z_r}\right) \cdot z \in U_x.$$

Clearly, $z'_r = 0$ and hence $U_x = \left\langle\{v, z'\}\right\rangle$. Thus, w.l.o.g we assume $z_r = 0$ and we may write $z = \sum_{i\in[n-1]} a_i z^i$ for some $a_i \in \mathbb{F}_q$, $i \in [n-1]$. Since $U_x = \langle\{v, z\}\rangle$ it follows that the 1-subspace $P(U_x)$ is spanned by the vector $\left(\det_{(s,t)} \binom{v}{z}\right)_{\{s,t\}\subseteq[n]}$. Hence, there exists some $\lambda \in \mathbb{F}_q$ such that:

$$\begin{aligned}
x_{\{s,t\}} &= \lambda \cdot \det_{(s,t)} \binom{v}{z} = \lambda(v_s z_t - v_t z_s) \\
&= \lambda \left(v_s \cdot \sum_{i\in[n-1]} a_i z_t^i - v_t \cdot \sum_{i\in[n-1]} a_i z_s^i \right) \quad \text{since } z = \sum_{i\in[n-1]} a_i z^i \\
&= \lambda \sum_{i\in[n-1]} a_i \left(v_s z_t^i - v_t z_s^i \right) \\
&= \lambda \sum_{i\in[n-1]} a_i p^i_{\{s,t\}} \quad \text{by (1)}.
\end{aligned}$$

Therefore $x \in \left\langle\{p^1, \dots, p^{n-1}\}\right\rangle$ which implies that $P_V \subseteq \left\langle\{p^1, \dots, p^{n-1}\}\right\rangle$. Thus we have proved that $P_V = \left\langle\{p^1, \dots, p^{n-1}\}\right\rangle$, and as a consequence we have that $P_V \in \mathcal{G}_q(n_2, n-1)$. □

Proof (*of* Theorem 15)**.** Let $\mathbb{C} \subseteq \mathcal{G}_q(n_2, n-1)$ be the code defined by

$$\mathbb{C} = \{P_V \mid V \in \mathcal{G}_q(n, 1)\}.$$

By Lemma 3, for each $V \in \mathcal{G}_q(n, 1)$ we have that P_V is an $(n-1)$-subspace of $\mathbb{F}_q^{n_2}$ and hence $\mathbb{C}$ is well-defined. By Lemma 1 and the discussion on $\mathcal{S}_{q,n}$, it follows that $\mathbb{C}$ is an 1-intersecting equidistant code. □

Remark 1. After the paper was written, we found that Lemma 3 can also be obtained as a consequence of [21, Theorem 24.2.9, p. 113] which discusses the theory of finite projective geometries. But, the proof of this Theorem requires more detailed theory which precedes it, while our proof is much shorter, simpler, and direct.

3.2. Do larger equidistant codes exist?

It was believed (Conjecture 1) that the largest non-sunflower 1-intersecting code in $\mathcal{G}_q(n, k)$ has size at most $\begin{bmatrix} k+1 \\ 1 \end{bmatrix}_q$. The following example consists of a non-sunflower 1-intersecting code $\mathbb{C} \subseteq \mathcal{G}_2(6, 3)$ of size 16, while $\begin{bmatrix} 4 \\ 1 \end{bmatrix}_2 = 15$. $\mathbb{C}$ was found by a computer search.

Let α be a primitive root of $x^6 + x + 1$, and use this primitive polynomial to generate $\mathbb{F}_2^6$. Let $\mathbb{C}$ be the code which consists of the following sixteen 3-subspaces:

$$\begin{array}{llll}
\left\langle\{\alpha^0, \alpha^1, \alpha^2\}\right\rangle & \left\langle\{\alpha^{10}, \alpha^{26}, \alpha^{25}\}\right\rangle & \left\langle\{\alpha^{12}, \alpha^9, \alpha^{29}\}\right\rangle & \left\langle\{\alpha^6, \alpha^5, \alpha^{33}\}\right\rangle \\
\left\langle\{\alpha^0, \alpha^{15}, \alpha^{10}\}\right\rangle & \left\langle\{\alpha^{18}, \alpha^1, \alpha^{59}\}\right\rangle & \left\langle\{\alpha^{25}, \alpha^0, \alpha^{58}\}\right\rangle & \left\langle\{\alpha^{19}, \alpha^{10}, \alpha^6\}\right\rangle \\
\left\langle\{\alpha^6, \alpha^{52}, \alpha^{51}\}\right\rangle & \left\langle\{\alpha^{33}, \alpha^{20}, \alpha^{59}\}\right\rangle & \left\langle\{\alpha^{41}, \alpha^2, \alpha^{36}\}\right\rangle & \left\langle\{\alpha^{58}, \alpha^6, \alpha^{49}\}\right\rangle \\
\left\langle\{\alpha^{12}, \alpha^{54}, \alpha^{15}\}\right\rangle & \left\langle\{\alpha^{49}, \alpha^{26}, \alpha^{46}\}\right\rangle & \left\langle\{\alpha^{36}, \alpha^{34}, \alpha^{30}\}\right\rangle & \left\langle\{\alpha^{36}, \alpha^{29}, \alpha^{26}\}\right\rangle.
\end{array}$$

3.3. Large non-sunflower equidistant codes

In this subsection, we will consider the construction of the largest t-intersecting codes in $\mathcal{G}_q(n, k)$. For n large enough this code is a sunflower and hence for such large n we will consider also the largest t-intersecting code which is not a sunflower.

By Theorem 1, sunflowers are the largest constant dimension equidistant codes when the ambient space is large enough. The size of the largest sunflower is usually not known, but we know that it is equal to the size of a related partial spread. Therefore, we would like to know what is the size of the largest t-intersecting code in $\mathcal{G}_q(n, k)$ which is not a sunflower.

Assume we want to generate a $(k-r)$-intersecting code in $\mathcal{G}_q(n, k)$. Clearly we must have $n \geq k + r$. If $k - r = 0$ then any $(k-r)$-intersecting code is a partial spread and hence also a sunflower. Therefore, we assume that $k - r > 0$. We start with the largest partial spread $\mathbb{S}$ in $\mathcal{G}_q(k + r, r)$. By Theorem 5, its size m is at least $q^k + 1$. $\mathbb{S}^\perp$ is a non-sunflower $(k-r)$-intersecting code in $\mathcal{G}_q(k + r, k)$ whose size m is at least $q^k + 1$. If $k - r > 1$ then we do not know how to construct a larger code. If $k - r = 1$ then larger codes of size $\frac{q^{k+1}-1}{q-1}$ are constructed in Section 3.1.

3.4. Equidistant codes in $\mathcal{P}_q(n)$

So far we have considered only constant dimension equidistant codes. Can we get larger unrestricted subspace equidistant codes over $\mathbb{F}_q^n$ than constant dimension equidistant codes over $\mathbb{F}_q^n$? We start by considering first equidistant codes in the Hamming scheme. Let $B_q(n, d)$ be the maximum size of an equidistant code of length n and minimum Hamming distance d over $\mathbb{F}_q$. Let $B_q(n, d, w)$ be the maximum size of an equidistant code of length n, constant weight w, and minimum Hamming distance d. The following result, due to [14] shows that when discussing equidistant codes in the Hamming scheme, we may restrict our attention to constant weight codes:

Theorem 16. $B_q(n, d) = 1 + B_q(n, d, d)$.

A related q-analog theorem might hold in some cases, but generally it does not hold as demonstrated in the following example. The example is specific in some sense, but it can be generalized to many other parameters.

Let n be an odd integer for which the largest 2-intersecting equidistant code in $\mathcal{G}_2(n, 4)$ with minimum subspace distance 4 is a sunflower. The size of the largest partial 2-spread in $\mathcal{G}_2(n-2, 2)$ is $\frac{2^{n-2}-4}{3}$. Let $\mathbb{C}$ be such a partial spread. Clearly, $\mathcal{E}^2(\mathbb{C})$ is the largest 2-intersecting equidistant code in $\mathcal{G}_2(n, 4)$. Let x, y, z, and u be the only nonzero vectors of $\mathbb{F}_2^{n-2}$ which do not appear in any 2-subspace of $\mathbb{C}$. Let $v_1 = (\mathbf{0}, 01)$, $v_2 = (\mathbf{0}, 10)$ be two vectors in $\mathbb{F}_2^n$ and let $\mathcal{E}^2(\mathbb{C}) = \{\langle (X, 00) \cup \{v_1, v_2\}\rangle \mid X \in \mathbb{C}\}$, where $(X, 00) = \{(x, 00) \mid x \in X\}$. The code

$$\mathbb{C}' = \mathcal{E}^2(\mathbb{C}) \bigcup \{\langle (\mathbf{0}, 01), (y, 11)\rangle, \langle (\mathbf{0}, 10), (z, 11)\rangle, \langle (\mathbf{0}, 11), (x, 11)\rangle\}$$

is an equidistant code in $\mathcal{P}_2(n)$ whose size is $\frac{2^{n-2}+5}{3}$ and its subspace distance is 4. This code is larger than $\mathcal{E}^2(\mathbb{C})$, which implies that q-analog of Theorem 16 does not exist in general.

4. Equidistant rank metric codes

In this section, we present a connection between the construction presented in Section 3.1 and equidistant rank-metric codes. To the best of our knowledge, this is the first construction of an equidistant rank metric code whose matrices are not of full rank.

In this section we use a *variant* of the function P, defined in Section 3.1, denoted by φ. This variant may be considered as acting on matrices from $\mathbb{F}_q^{k\times n}$ rather than on $\mathcal{G}_q(n, k)$, and maps them to $\mathbb{F}_q^{n_k}$ rather than to $\mathbb{P}_q^{n_k-1}$.

Definition 1. Given $M \in \mathbb{F}_q^{k\times n}$, identify the coordinates of $\mathbb{F}_q^{n_k}$ with k-subsets of $[n]$, and define $\varphi(M)$ as a vector of length $n_k = \binom{n}{k}$ with:

$$(\varphi(M))_{(i_1,\ldots,i_k)} = \det M\,(i_1, \ldots, i_k)$$

where $M\,(i_1, \ldots, i_k)$ is the $k \times k$ sub-matrix of M formed from columns $i_1, \ldots, i_k$ of M.

For $v, u \in \mathbb{F}_q^n$ denote $X_{v,u} = \varphi\binom{v}{u}$. For $v \in \mathbb{F}_q^n \setminus \{0\}$, define:

$$M_v = \begin{pmatrix} X_{v,e_1} \\ \vdots \\ X_{v,e_n} \end{pmatrix},$$

where e_i is a unit vector of length n. Let $\mathbb{M} = \langle \{M_{e_1}, \ldots, M_{e_n}\}\rangle$. In the rest of this section we prove that $\mathbb{M}\setminus\{0\}$ is an equidistant constant rank code of size $q^n - 1$.

The following lemma shows that for $k = 2$, the function φ is *linear* in some sense, when one of the vectors in the matrix it operates on is fixed.

Lemma 4. *If $u, v, w \in \mathbb{F}_q^n$ and $\alpha, \beta \in \mathbb{F}_q$ then $X_{v,\alpha u+\beta w} = \alpha \cdot X_{v,u} + \beta \cdot X_{v,w}$. Similarly, $X_{\alpha u+\beta w,v} = \alpha \cdot X_{u,v} + \beta \cdot X_{w,v}$.*

Proof. Consider the $\{s, t\}$ coordinate of the vector $\alpha \cdot X_{v,u} + \beta \cdot X_{v,w}$:

$$\begin{aligned}
\left(\alpha \cdot X_{v,u} + \beta \cdot X_{v,w}\right)_{\{s,t\}} &= \alpha\,(v_s u_t - v_t u_s) + \beta\,(v_s w_t - v_t w_s) \\
&= v_s\,(\alpha u_t + \beta w_t) - v_t\,(\alpha u_s + \beta w_s) \\
&= v_s\,(\alpha u + \beta w)_t - v_t\,(\alpha u + \beta w)_s \\
&= \left(\varphi\begin{pmatrix} v \\ \alpha u + \beta w\end{pmatrix}\right)_{\{s,t\}} \\
&= \left(X_{v,\alpha u+\beta w}\right)_{\{s,t\}}.
\end{aligned}$$

The claim that $X_{\alpha u+\beta w,v} = \alpha \cdot X_{u,v} + \beta \cdot X_{w,v}$ has a similar proof. □

Corollary 4. *If $V \in \mathcal{G}_q(n,1)$ and $v \in V \setminus \{0\}$ then $P_V = \left\langle \{X_{v,z^1}, \dots, X_{v,z^{n-1}}\} \right\rangle$, where z^i, $i \in [n-1]$ was defined in Lemma 3.*

We now show that each nonzero codeword in $\mathbb{M}$ can be written as M_v for some $v \in \mathbb{F}_q^n$, where $rank(M_v) = n-1$. Hence, the linearity of the code implies that the rank of the difference between any two matrices in the code is $n-1$, and therefore the code is equidistant.

Lemma 5. $\mathbb{M} = \left\{ M_v | v \in \mathbb{F}_q^n \right\}$.

Proof. Let $M = \sum_{i=1}^n \alpha_i M_{e_i} \in \mathbb{M}$, for some $\alpha_i \in \mathbb{F}_q$, $i \in [n]$. By Lemma 4, the jth row of M is:

$$\sum_{i=1}^n \alpha_i X_{e_i,e_j} = X_{(\sum_{i=1}^n \alpha_i e_i),e_j} = X_{v,e_j},$$

where $v = \sum_{i=1}^n \alpha_i e_i$, and therefore $M = M_v$. Conversely, let $v = \sum_{i=1}^n \alpha_i e_i$. The same arguments (in reversed order) show that $M_v = \sum_{i=1}^n \alpha_i M_{e_i}$ and hence $M_v \in \mathbb{M}$. □

Lemma 6. *If $v = \sum_{i=1}^n \alpha_i e_i,\ \alpha_i \in \mathbb{F}_q, i \in [n]$ is a non-zero vector in $\mathbb{F}_q^n$ then $rank(M_v) = n-1$.*

Proof. By Corollary 4, the rows of M_v contain a basis for the codeword $P_{\langle v \rangle}$ (following the notations of Theorem 15). Recall (see Lemma 3) that a basis for $P_{\langle v \rangle}$ is obtained by omitting one vector from the set $\left\{ X_{v,e_1}, \dots, X_{v,e_n} \right\}$. Note that r is the index of the omitted vector and $\alpha_r \neq 0$ (see Lemma 3). To complete the proof, we have to show that the vector X_{v,e_r} lies inside $P_{\langle v \rangle}$. Notice that by Lemma 3 we have that $\alpha_r \neq 0$. We have that

$$\begin{aligned}
\sum_{i \in [n] \setminus \{r\}} \alpha_i X_{v,e_i} &= \varphi \begin{pmatrix} v \\ \sum_{i \in [n] \setminus \{r\}} \alpha_i e_i \end{pmatrix} \\
&= \varphi \begin{pmatrix} v \\ v - \alpha_r e_r \end{pmatrix} \\
&= \varphi \begin{pmatrix} v \\ -\alpha_r e_r \end{pmatrix} \\
&= -\alpha_r \varphi \begin{pmatrix} v \\ e_r \end{pmatrix} = -\alpha_r X_{v,e_r}.
\end{aligned}$$

Therefore, $X_{v,e_r} = -\frac{1}{\alpha_r} \sum_{i \in [n] \setminus \{r\}} \alpha_i X_{v,e_i}$. Thus, rowspan $(M_v) = P_{\langle v \rangle}$ and $rank\,(M_v) = \dim P_{\langle v \rangle} = n-1$. □

Lemma 7. *If $M_v = M_u$ for $u, v \in \mathbb{F}_q^n$ then $u = v$.*

Proof. If $M_u = M_v$ then $X_{v,e_j} = X_{u,e_j}$ for all $j \in [n]$, which implies

$$\forall j \in [n],\ \forall \{s,t\} \in \binom{[n]}{2}, \quad v_s e_{j,t} - v_t e_{j,s} = u_s e_{j,t} - u_t e_{j,s}. \tag{3}$$

In particular, for any $i \in [n] \setminus \{j\}$ we may choose $s = i$, $t = j$ and obtain that $v_i = u_i$. Since (3) holds for any $j \in [n]$, we also have $v_j = u_j$ and thus $u = v$. □

Corollary 5. $|\mathbb{M}| = q^n$.

Corollary 6. *$\mathbb{M} \setminus \{0\}$ is an equidistant constant rank code over $\mathbb{F}_q$ with matrices of size $n \times \binom{n}{2}$, rank $n-1$, rank distance $n-1$, and size $q^n - 1$.*

There is some similarity between the code $\mathbb{M}$ and the Sylvester's type Hadamard matrix of order 2^n [25]. This code is a binary linear of dimension n and length 2^n. Each codeword, except for the all zeros codeword has weight 2^{n-1} and the mutual Hamming distance between any two codewords in 2^{n-1}. The analog to the code $\mathbb{M}$ seems to be obvious.

5. Recursive construction of equidistant subspace codes

We have shown in Section 3.1 a direct construction of an 1-intersecting code in $\mathcal{G}_q(n_2, n-1)$. In this section, we prove that this code can be constructed recursively, by using some of the results of Section 4.

Let $\mathbb{C}_{n-1}, \mathbb{C}_n$ be the 1-intersecting codes in $\mathcal{G}_q\left(\binom{n-1}{2}, n-2\right), \mathcal{G}_q\left(\binom{n}{2}, n-1\right)$, respectively, as constructed in Section 3.1. We first present a construction of *some* code $\mathbb{D} \subseteq \mathcal{G}_q\left(\binom{n}{2}, n-1\right)$ from $\mathbb{C}_{n-1}$ and later prove that $\mathbb{D} = \mathbb{C}_n$.

Let $\hat{v} \in \mathbb{F}_q^{n-1} \setminus \{0\}$. For the purpose of the construction, let $X_{\hat{v},\hat{e}_i} = \varphi\begin{pmatrix} \hat{v} \\ \hat{e}_i \end{pmatrix}$ as in Section 4 ($\hat{e}_i$ is a unit vector of length $n-1$), and let $\mathcal{B}_{\hat{v}} = \{\hat{z}^1, \ldots, \hat{z}^{n-2}\}$ be the set of $n-2$ unit vectors of length $n-1$ such that $P_{\langle \hat{v} \rangle} = \langle \{X_{\hat{v},\hat{z}^1}, X_{\hat{v},\hat{z}^2}, \ldots, X_{\hat{v},\hat{z}^{n-2}}\} \rangle$, as denoted in the proof of Lemma 3. For $v \in \mathbb{F}_q^n \setminus \{0\}$ we define e_i, X_{v,e_i} and $\mathcal{B}_v$ similarly.

For each codeword $P_{\langle \hat{v} \rangle} \in \mathbb{C}_{n-1}$ we construct q codewords in $\mathbb{D}$, denoted by $\{U_{\hat{v},a}\}_{a \in \mathbb{F}_q}$, as follows:

$$U_{\hat{v},0} = \text{rowspan}\begin{pmatrix} \hat{v} & \mathbf{0} \\ \mathbf{0} & X_{\hat{v},\hat{z}^1} \\ \vdots & \vdots \\ \mathbf{0} & X_{\hat{v},\hat{z}^{n-2}} \end{pmatrix}$$

$$\forall a \neq 0,\; U_{\hat{v},a} = \text{rowspan}\left(I_{(n-1)\times(n-1)} \left| \begin{matrix} a \cdot X_{\hat{v},\hat{e}_1} \\ \vdots \\ a \cdot X_{\hat{v},\hat{e}_{n-1}} \end{matrix} \right. \right).$$

In addition, we add a codeword $U_0 = \text{rowspan}\left(I_{(n-1)\times(n-1)} | \mathbf{0}\right)$ to $\mathbb{D}$.

Theorem 17. $\mathbb{D} = \mathbb{C}_n$.

Proof. We prove that any $P_{\langle v \rangle} \in \mathbb{C}_n$ is equal to some codeword in $\mathbb{D}$. The equality, $\mathbb{D} = \mathbb{C}_n$, will follow since $|\mathbb{D}| \leq |\mathbb{C}_{n-1}| \cdot q + 1 = \begin{bmatrix} n-1 \\ 1 \end{bmatrix}_q \cdot q + 1 = \begin{bmatrix} n \\ 1 \end{bmatrix}_q = |\mathbb{C}_n|$. Let $P_{\langle v \rangle} \in \mathbb{C}_n$ for $v \in \mathbb{F}_q^n \setminus \{0\}$, and let $v = (a, \hat{u}) \neq (0, \mathbf{0})$, where $a \in \mathbb{F}_q$, $\hat{u} \in \mathbb{F}_q^{n-1}$. To find the related codeword in $\mathbb{D}$, we distinguish between the following three cases:

Case 1. $a = 0$. W.l.o.g we choose $\mathcal{B}_v$ such that $z^1 = e_1$, where e_1 is a unit vector of length n. We have that $X_{v,z^1} = (-\hat{u}, \mathbf{0})$, where $\mathbf{0}$ is the all zeros vector of length $\binom{n-1}{2}$; for all $z^i \in \mathcal{B}_v$, $2 \leq i \leq n-1$ we have that $X_{v,z^i} = (\mathbf{0}, X_{\hat{u},\hat{z}^i})$, where $\hat{z}^i$ is the $(n-1)$-suffix of $\hat{z}^i$ and $\mathbf{0}$ is the all zeros vector of length $n-1$. Hence, Corollary 4 implies that $P_{\langle v \rangle} = \langle \{X_{v,z^1}, \ldots, X_{v,z^{n-1}}\} \rangle = U_{\hat{u},0}$.

Case 2. $a \neq 0$, $u \neq \mathbf{0}$. For $i \geq 2$ we have:

$$X_{v,e_i} = \Bigg(\underbrace{0, \ldots, 0, a, 0, \ldots, 0}_{n-1 \text{ entries, } (i-1)\text{th equals } a}, \qquad \underbrace{X_{\hat{u},\hat{e}_{i-1}}}_{\binom{n-1}{2} \text{ entries}} \Bigg),$$

where $\hat{e}_{i-1}$ is the $(n-1)$-suffix of the unit vector $e_i \in \mathbb{F}_q^n$. Since $a \neq 0$ we may choose $\mathcal{B}_v = \{e_2, \ldots, e_n\}$ and obtain by Corollary 4 that $P_{\langle v \rangle} = \langle \{X_{v,e_2}, \ldots, X_{v,e_n}\} \rangle = U_{u,a^{-1}}$.

Case 3. $a \neq 0$, $u = \mathbf{0}$. For $i \geq 2$ we have:

$$X_{v,e_i} = \Bigg(\underbrace{0, \ldots, 0, a, 0, \ldots, 0}_{n-1 \text{ entries, } (i-1)\text{th equals } a}, \mathbf{0} \Bigg).$$

We may similarly choose $\mathcal{B}_v = \{e_2, \ldots, e_n\}$ and obtain $P_{\langle v \rangle} = U_0$.

Starting from an 1-intersecting code in $\mathcal{G}_q(3, 2)$ which consists of all the two-dimensional subspaces of $\mathbb{F}_q^3$ we can obtain all the codes constructed in Section 3 recursively. We note that the initial condition consists exactly of all the lines of the projective plane of order q.

6. Conclusion and problems for future research

We have made a discussion on the size of the largest t-intersecting equidistant codes. The largest codes are known to be the trivial sunflowers. We discussed trivial codes and surveyed the known results in this direction. A construction of non-sunflower 1-intersecting codes in $\mathcal{G}_q(n, k)$, $n \geq \binom{k+1}{2}$, whose size is $\begin{bmatrix} k+1 \\ 1 \end{bmatrix}_q$, based on the Plücker embedding, is given. We showed that in at least one case there are larger non-sunflower 1-intersecting equidistant codes. Many important and usually very difficult problems remained for future research. We list herein a few.

1. Find the size of the largest partial spread for any given set of parameters.
2. Prove (or disprove) that the size of a non-sunflower t-intersecting constant dimension code of dimension k, where $t > 1$ and $k > t + 1$, is at most $\begin{bmatrix} k+1 \\ 1 \end{bmatrix}_q$.

3. Identify the cases for which the size of a non-sunflower t-intersecting constant dimension code of dimension k, where $t > 1$ and $k > t + 1$, is less than $\begin{bmatrix} k+1 \\ 1 \end{bmatrix}_q$.
4. Identify the cases for which the size of a non-sunflower 1-intersecting constant dimension code of dimension k, where $k > 2$, is greater than $\begin{bmatrix} k+1 \\ 1 \end{bmatrix}_q$.
5. Find new constructions for non-sunflower t-intersecting constant dimension codes of dimension k, where $t \geq 1$, $k > t + 1$, whose size is larger than the codes obtained from partial spreads and their orthogonal codes.
6. Prove or disprove that the size of the largest equidistance code with subspaces distance d in $\mathcal{P}_q(n)$ depends on the size of the largest equidistance code with subspace distance d in $\mathcal{G}_q(n, k)$ for some k.
7. Find 1-intersecting codes in $\mathcal{G}_q(n, k)$ of size $\begin{bmatrix} k+1 \\ 1 \end{bmatrix}_q$, $k > 3$ and $n < \binom{k+1}{2}$.
8. Develop the theory of constant rank codes.
9. Find large equidistant rank metric codes.

Acknowledgment

This research was supported in part by the Israel Science Foundation (ISF), Jerusalem, Israel, under Grant 10/12. The work of Netanel Raviv is part of his Ph.D. thesis performed at the Technion.

References

[1] A. Beutelspacher, Partial spreads in finite projective spaces and partial designs, Math. Z. 145 (1975) 211–229.
[2] A. Beutelspacher, U. Rosenbaum, Projective Geometry: From Foundations to Applications, Cambridge University Press, Cambridge, 1998.
[3] M. Braun, T. Etzion, A. Vardy, Linearity and complements in projective space, Linear Algebra Appl. 438 (2013) 57–70.
[4] A. Chowdhury, personal communication (see also Shadows and intersections in vector spaces, http://ima.umn.edu/~ameera/research/shadow-int-vec-space-extended.pdf 2009).
[5] P. Delsarte, Bilinear forms over a finite field, with applications to coding theory, J. Combin. Theory Ser. A 25 (1978) 226–241.
[6] M. Deza, Une propriété extrémale des plans projectifs finis dans une classe de codes equidistants, Discrete Math. 6 (1973) 343–352.
[7] M. Deza, P. Frankl, Every large set of equidistant $(0, +1, -1)$-vectors forms a sunflower, Combinatorica 1 (1981) 225–231.
[8] D.A. Drake, J.W. Freeman, Partial t-spreads and group constructible (s, r, μ)-nets, Journal of Geom. 13 (1979) 210–216.
[9] S. El-Zanati, H. Jordon, G. Seelinger, P. Sissokho, L. Spence, The maximum size of a maximal 3-spread in a finite vector space over GF(2), Des. Codes Cryptogr. 54 (2010) 101–107.
[10] P. Erdös, C. Ko, R. Rado, Intersection theorems for systems of finite sets, Q. J. Math. Oxford 12 (1961) 313–320.
[11] T. Etzion, N. Silberstein, Error-correcting codes in projective space via rank-metric codes and Ferrers diagrams, IEEE Trans. Inform. Theory 55 (2009) 2909–2919.
[12] T. Etzion, A. Vardy, Error-correcting codes in projective space, IEEE Trans. Inform. Theory 57 (2011) 1165–1173.
[13] P. Frankl, R.M. Wilson, The Erdös-Ko-Rado theorem for vector spaces, J. Combin. Theory Ser. A 43 (1986) 228–236.
[14] F. Fu, T. Kløve, Y. Luo, V.K. Wei, On equidistant constant weight codes, Discrete Appl. Math. 128 (2003) 157–164.
[15] E.M. Gabidulin, Theory of codes with maximum rank distance, Probl. Inf. Transm. 21 (1985) 1–12.
[16] M. Gadouleau, Z. Yan, Constant-rank codes and their connection to constant-dimension codes, IEEE Trans. Inform. Theory 56 (2010) 3207–3216.
[17] J.I. Hall, Bounds for equidistant codes and partial projective planes, Discrete Math. 17 (1977) 85–94.
[18] J.I. Hall, A.J.E.M. Jansen, A.W.J. Kolen, J.H. Van Lint, Equidistant codes with distance 12, Discrete Math. 17 (1977) 71–83.
[19] J.P. Hansen, Osculating spaces of varieties and linear network codes, in: Algebraic Informatics, Springer, Berlin, Heidelberg, 2012, pp. 83–88.
[20] J.P. Hansen, Forms and linear network codes, arXiv:1303.1626, 2013.
[21] J.W.P. Hirschfeld, J.A. Thas, General Galois Geometries, vol. 1378, Clarendon Press Oxford, 1991.
[22] S.J. Hong, A.M. Patel, A general class of maximal codes for computer applications, IEEE Trans. Comput. 21 (1972) 1322–1331.
[23] W.N. Hsieh, Intersection theorems for systems of finite vector spaces, Discrete Math. 12 (1975) 1–16.
[24] R. Koetter, F.R. Kschischang, Coding for errors and erasures in random network coding, IEEE Trans. Inform. Theory 54 (2008) 3579–3591.
[25] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland Press, Amsterdam, 1977.
[26] J. Rosenthal, N. Silberstein, A.L. Trautmann, On the geometry of balls in the Grassmannian and list decoding of lifted Gabidulin codes, Des. Codes Cryptogr. 73 (2014) 393–416.
[27] J. Rosenthal, A.L. Trautmann, Decoding of subspace codes, a problem of schubert calculus over finite fields, arXiv:1209.2887, 2012.
[28] R.M. Roth, Maximum-rank array codes and their application to crisscross error correction, IEEE Trans. Inform. Theory 37 (1991) 328–336.
[29] D. Silva, F.R. Kschischang, R. Koetter, A rank-metric approach to error control in random network coding, IEEE Trans. Inform. Theory 54 (2008) 3951–3967.
[30] S.-T. Xia, F.-W. Fu, Johnson type bounds on constant dimension codes, Des. Codes Cryptogr. 50 (2009) 163–172.