Two-weight code using the geometry $D_{n,k}$

Dr. Abdelsalam Osman Abou Zayda*

الملخص

نستخدم في هذا البحث هندسة نقطة–خط من نوع $D_{n,k}$ لانشاء رمز ثنائي الوزن. الوزن الأول لذلك الرمز يأتي من وجود symplecta من نوع $A_{3,2}$ والوزن الثاني يأتي من وجود symplecta من نوع $D_{n-k+1,1}$.

Abstract

In this paper we use the point-line geometry of type Dn,k(F) to construct a binary two-weight code. The first weight of the code comes from the existance of symlecta of type A3,2 and the second weight comes from the existence of symplecta of type Dn-k+1,1.

Key words: Hamming distance, Hamming weight, Hyperbolic geometry.

* **Assist. Professor in Mathematics, Mathematics Department, Al-Aqsa University, Gaza, Palestine**

E-mail : salamelden@hotmail.com

1. Introduction

In recent year there has been an increasing interest in finite spaces, and important applications to practical topics such as coding theory. Many authors have interested in some type of codes called constant-weight codes, tables of upper and lower bounds where constructed for the sizes of a given minimal distances and a given length, see [1-3].

Many papers have taken the algebraic concepts for purpose of obtaining codes, here we used the geometric means to construct some families of binary non-collinear two-weight codes, at the same time there are many geometries that can be used to construct such codes. In [7] EL-Atrash used this method by defining the non-linear binary constant-weight code that arises from the Half-spin geometry $D_{5,5}$.

A subspace of a point-line geometry Γ=(P, L) is a subset $X \subseteq P$ such that any line which has at least two of its incident points in X has all of its incident points in X. $\langle X \rangle$ means the intersection over all subspaces containing X, where $X \subseteq P$. Lines incident with more than two points are called *thick* lines, those incident with exactly two points are called *thin* lines.

$x^{\perp}$ means the set of all points in P collinear with x, including x itself. ***A clique*** of P is a set of points in which every pair of points are collinear. ***A partial linear*** space is a point-line geometry (P, L), in which every pair of points are incident with at most one line, and all lines have cardinality at least 2. A point line geometry Γ=(P, L) is called ***singular*** or (***linear***) if every pair of points are incident with a unique line.

The singular rank of a space Γ is the maximal number n (possibly ∞) for which there exist a chain of distinct subspaces $\varnothing \neq X_0 \subset X_1 \subset ... \subset X_n$ such that X_i is singular for each i, $X_i \neq X_j$, $i \neq j$, for example rank($\varnothing$) =-1, rank({p})=0 where p is a point and rank(L)=1 where L a line.

In a point-line geometry Γ=(P, L), ***a path of length*** n is a sequence of n+ 1 $(x_0, x_1,..,x_n)$ where, (x_i,x_{i+1}) are collinear, x_0 is called the initial point and x_n is called the end point. ***A geodesic*** from a point x to a point y is a path of minimal possible length with initial point x and end point y. We denote this length by $d_\Gamma(x, y)$.

A geometry Γ is called ***connected*** if and only if for any two of its points there is a path connecting them. A subset X of P is said to be ***convex*** if X contains all points of all geodesics connecting two points of X.

A gamma space is a point-line geometry such that for every point-line pair (p, *l*), p is collinear with either no point, exactly one point, or all points of *l*, i.e., $p^{\perp} \cap l$ is empty, consists of a single point, or l.

A polar space is a point-line geometry Γ=(P, L) satisfying the Buekenhout-Shult axiom:
For each point-line pair (p, *l*) *with p not incident with l; p is collinear with one or all points of l, that is* $|p^{\perp} \cap l| = 1$ *or else* $p^{\perp} \supset l$. Clearly this axiom is equivalent to saying that $p^{\perp}$ is a geometric hyperplane of Γ for every point $p \in P$.

A point-line geometry Γ=(P, L) is called ***a projective plane*** if and only if it satisfies the following conditions:

(i) Γ is a linear space; every two distinct points x, y in P lie exactly on one line,

(ii) every two lines intersect in one point,

(iii) there are four points no three of them are on a line.

A point-line geometry Γ=(P, L) is called ***a projective space*** if the following conditions are satisfied:

(i) every two points lie exactly on one line ,

(ii) if l_1, l_2 are two lines $l_1 \cap l_2 \neq \emptyset$, then $\langle l_1, l_2 \rangle$ is a projective plane. ($\langle l_1, l_2 \rangle$ means the smallest subspace of Γ containing l_1 and l_2.)

A point-line geometry Γ=(P, L) is called ***a parapolar space*** if and only if it satisfies the following properties:

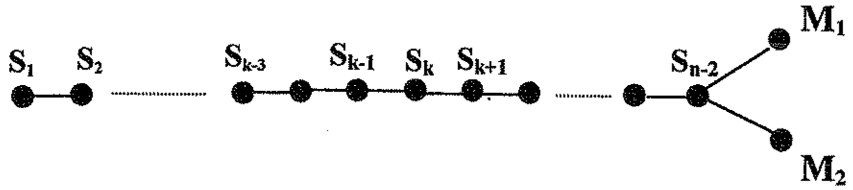
(i) Γ is a connected gamma space,

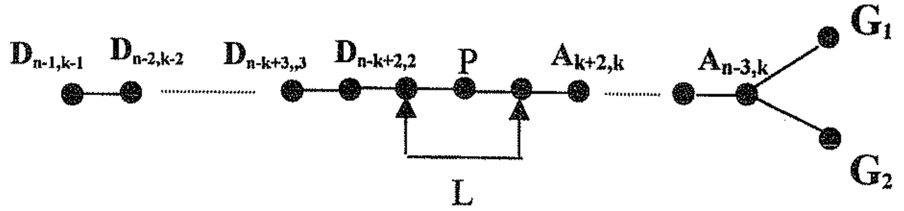
(ii) for every line *l*; $l^{\perp}$ s not a singular subspace,

(iii) for every pair of non-collinear points x, y; $x^{\perp} \cap y^{\perp}$ is either empty, a single point, or a non-degenerate polar space of rank at least 2.

If x, y are distinct points in P, and if $|x^{\perp} \cap y^{\perp}|=1$, then (x, y) is called ***a special pair***, and if $x^{\perp} \cap y^{\perp}$ is a polar space, then (x, y) is called ***a polar pair*** (or ***a symplectic pair***). A parapolar space is called ***a strong parapolar*** space if it has no special pairs

3- Construction of $D_{n,k}$ (F) [10]. Consider the polar space $\Delta = \Omega^{+}(2n, F)$ that comes from a vector space V of dimension 2n over a finite field F=GF(*q*) with a symmetric hyperbolic bilinear form B. $\mathbf{S_I}$ is the set of all totally isotropic i-dimensional subspaces of V; $1 \leq i \leq n-2$. The two classes $\mathbf{M_1}$, $\mathbf{M_2}$ consist of maximal totally isotropic n-dimensional subspaces. Two n-spaces fall in the same class if their intersection is of odd dimension.





$D_{n,k}(F)$

The geometry of type **$D_{n,k}(F)$** is the point-line geometry (P, L), whose set of points P is the collection of all k-dimensional subspaces of the vector space V, and whose lines are the pairs (A, B) where A is (k-1)-dimensional subspace of (k+1)-subspace B–that is, the set of (k-1, k+1)-subspace of V. A point C is incident with a line (A, B) if and only if $A \subset C \subset B$ as a subspaces of V.

To define the collinearity, let C_1 and C_2 be two point (the points are the T.I k-spaces), then C_1 is collinear to C_2 if and only if the intersection of $C_1 \cap C_2$=(k-1)-space and $\langle C_1, C_2 \rangle$=(k+1)-space.

The elements of the classes **G_1** and **G_2** are Grassmannian geometries of type **$A_{n-1,k}$**.

There are two kinds of symlecta (1) The first kind is the convex polar spaces $A_{3,2}$ that represent the (k-2, k+2) subspaces of V. Then symplecton S of kind $A_{3,2}$ is the set of TI k-dimensional spaces that contain the TI (k-2)-dimensional space and contained in the TI (k+2)-dimensional space. (2) The second kind of symplecta is the convex polar spaces of type $D_{n-k+1,1}$ that represent the collection of all TI (k-1)-subspaces of V. Thus this kind of symplecta is defined as the collection of all TI k-subspaces of V that contain such TI (k-1)-spaces.

The properties and their proofs of the geometry that will be mentioned below can be straightforward obtained from [10]

3.1 Proposition. *Let* Γ=(P, L) *be the geometry* of type $D_{n,k}(F)$. *Thus*:

i- Γ *is of diameter* k+1,.

ii- Γ *is parapolar geometry.*

3.2. Proposition [10]. *Let* Γ=(P, L) *be the geometry* of *type* $D_{n,k}(F)$ *for any field* F. *Then the following hold:*

1- If S_1 and S_2 are tow symplecta of type $A_{3,2}$, then rank($S_1 \cap S_2$)=-1, 0, 2.

2- If S_1 and S_2 are two symplecta of type $D_{n-k+1,1}$, then rank($S_1 \cap S_2$)=-1, 0.

3- If (p, S) is a non-incident pair of point and symplecta of type $A_{3,2}$, then $p^{\perp} \cap S$ is empty or projective plane. If a symplecton S is of type $D_{n-k+1,1}$, then $p^{\perp} \cap S$ is empty or a line.

4- Finite classical polar spaces

For more details about the finite classical polar space, see [5] and [9]. Let V be a vector space over a finite field F=GF(q), q is a prime power.

1- *Symplectic Geometry* $W_n(q)$ is the point-line geometry (P, L), where P is the set of all 1-dimensional subspaces ⟨x⟩ of V for which B(x, x)=0, and L is the set of all 2-dimensional subspaces ⟨x, y⟩ for which B(x, y)=0, for a symplectic bilinear form B. In this case n is even, the polar space is of rank n/2.

2- *Hypebolic Geometry* $\Omega^{+}(n, q)$ is the point-line geometry (P, L), where P is the set of all 1-dimensional subspaces ⟨x⟩ of V for which B(x, x)=0, and L is the set of all 2-dimensional ⟨x, y⟩ for which B(x, y)=0, for a hyperbolic bilinear form B. In this case n is even, the polar space is of rank n/2.

3- *Elliptic Geometry* $\Omega^{-}(n, q)$ is the point-line geometry (P, L), where P is the set of all 1-dimensional subspaces ⟨x⟩ of V for which B(x, x)=0, and L is the set of all 2-dimensional ⟨x, y⟩ for which B(x, y)=0, for elliptic bilinear form B.n In this case n is even, the polar space is of rank (n/2)-1.

4- *Orthogonal Geometry* $\Omega(n, q)$ is the point-line geometry (P, L), where P is the set of all 1-dimensional subspaces ⟨x⟩ of V for which B(x, x)=0, and L is the set of all 2-dimensional ⟨x, y⟩ for which B(x, y)=0, for orthogonal bilinear form B. In this case n is odd, the polar space is of rank n/2.

5- *Hermitian Geometry* $H^+_n(q^2)$ is the point-line geometry (P, L), where P is the set of all 1-dimensional subspaces ⟨x⟩ of V for which B(x, x)=0, and L is the set of all 2-dimensional ⟨x, y⟩ for which B(x, y)=0, for a Hermitian bilinear form B. In this case n is odd, the polar space is of rank (n-1)/2.

4.1 Theorem.[9,6]. The numbers of points of the finite classical polar spaces are given by the following formulae:

$$|W_{2n}(q)| = (q^{2n}-1)/(q-1),$$
$$|\Omega(2n+1,q)| = (q^{2n}-1)/(q-1),$$
$$|\Omega^+(2n,q)| = (q^{n-1}+1)(q^n-1)/(q-1),$$
$$|\Omega^-(2n,q)| = (q^{n-1}-1)(q^n+1)/(q-1),$$
$$|H^+(2n,q^2)| = (q^{2n}-1)(q^{2n}+1)/(q^2-1).$$

4.2 Theorem.[6,9]. The numbers of maximal totally singular subspaces of the finite classical polar spaces are given by the following formulae:

$$|\Sigma(W_{2n}(q))| = (q+1)(q^2+1)\ldots(q^{2n}+1),$$
$$|\Sigma(\Omega(2n+1,q))| = (q+1)(q^2+1)\ldots(q^{n+1}+1),$$
$$|\Sigma(\Omega^+(2n,q))| = 2(q+1)(q^2+1)\ldots(q^n+1),$$
$$|\Sigma(\Omega^-(2n,q))| = (q^2+1)(q^3+1)\ldots(q^n+1),$$
$$|\Sigma(H^+(2n,q^2))| = (q+1)(q^3+1)\ldots(q^n+1).$$

4.3 Proposition [5]. The number of subspaces of dimension k in a vector space of dimension n over GF(q) is

$$\frac{(q^n-1)(q^n-q)\ldots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\ldots(q^k-q^{k-1})}$$

Proof. This is the proof of Proposition 1.4.1 in [5].

Remark. This number is called a *Gaussian coefficient*, and is denoted by

$$\begin{bmatrix} n \\ k \end{bmatrix}.$$

4.4. Theorem [4]. Let V be equipped with a bilinear form then the number of Totally isotropic *k*-subspaces is the following:

in the symplectic case W(2*n*,*q*)

$$\begin{bmatrix} n \\ k \end{bmatrix}_q \prod_{i=0}^{k-1}(q^{n-i}+1)$$

$$\begin{bmatrix} n \\ k \end{bmatrix}_q \prod_{i=0}^{k-1}(q^{n-i}+1) \quad \text{in the orthogonal case } \Omega(2n+1,q).$$

$$\begin{bmatrix} n \\ k \end{bmatrix}_q \prod_{i=0}^{k-1}(q^{n-i-1}+1) \quad \text{in the hyperbolic case } \Omega^+(2n,q).$$

$$\begin{bmatrix} n \\ k \end{bmatrix}_q \prod_{i=0}^{k-1}(q^{n-i-1}+1) \quad \text{in the elliptic case } \Omega^-(2n+2,q).$$

Proof. see [4].

4.5 Corollary. Let (P, L) be the point-line geometry $D_{n,k}(F)$, F=GF(q) is a field, then the number of the Grassmannians of type $A_{n-1,k}$ of the classes G_1 and G_2 is $|\Sigma(\Omega^+(2n,q))|=2(q+1)(q^2+1)\dots(q^n+1)$.

5- Construction of the code

In this section we shall construct a binary two-weight code that is arising from the geometry $D_{n,k}(F)$. (For more detailed about the definitions in this section see [8]

A code C of length n and *size* M over a field F is just a subset of F^n of cardinality M, then we say that C is (n, M)-code.

Thus each code consists of "codwords" (vectors in F^n) and the number of codwords is the size of the code.

The *Hamming wieght* of $u=(x_1, x_2, \dots, x_n)$ is the number of non-zero coordinates x_i, i=1, 2, …, n, it is denoted by $w_h(u)$.

Let C be a code of length n and u, v be two codewords. The *hamming distance* between u and v, $d_h(u, v)$, is the number of coordinate in which they differ, that is $d_h(u,v)=w_h(u+v)$. If d= minimum $\{d_h(u,v):u, v\in C, u\neq v\}$; d is called the minimum distance of C, in this case we say that C is (n, M, d)-code. If C is a linear vector subspace of F^n, then C is called a *linear code* and if the dimension of C is k; we say that C is [n, k, d]-code. If all codewords in C have the same hamming weight w then C is called a *contant-wieght code*. An (n, M, d, w)-code is a constant-weight (n, M, d)-code with w as the common weight of all codewords. If the code C have two weights w_1 and w_2, then C is called *a two–weight code* (n, M, d, w_1, w_2).

5.1. Theorem. Let $p_1, p_2, \dots, p_s$ be the set of all points in $\Gamma=D_{n,k}(F)$. Let $S_1, S_2, \dots, S_t$ be the set of all symplecta in Γ of types $D_{n-k+1,1}$ and $A_{3,2}$. Let

$G=(g_{ij})$ be the incidence matrix, where $g_{ij}=1$ if the point p_j is incident with the symlecton S_i and $g_{ij}=0$ otherwise. Then the rows of G represent a non-linear binary two-weight code of parameters (n, M, d, w_1, w_2), where

$$n=\begin{bmatrix} n \\ k \end{bmatrix}_q \prod_{i=0}^{k-1}(q^{n-i-1}+1),$$

$$M=\begin{bmatrix} n \\ k-1 \end{bmatrix}_q \prod_{i=0}^{k-2}(q^{n-i-1}+1)+\begin{bmatrix} n \\ k+2 \end{bmatrix}_q \prod_{i=0}^{k+1}(q^{n-i-1}+1),$$

$$w_1= 2(q+1)(q^2+1)\ldots(q^{n-k+1}-1),$$

$$w_2=\begin{bmatrix} k+2 \\ k \end{bmatrix}_q \prod_{i=0}^{k-1}(q^{k-i+1}+1),$$

$$d=2(q^2+1)(q^3-1)/(q-1)-2\begin{bmatrix} k+1 \\ k \end{bmatrix}_q \prod_{i=0}^{k-1}(q^{k-i}+1).$$

Proof. Since there are two kinds of symplecta and each of them has different cardinality of 1's, then we have two-weight code. The number of columns of G is the number of distinct points, that are corresponding to the number of TI k-subspaces of V, then by Theorem 4.4 $n=\begin{bmatrix} n \\ k \end{bmatrix}_q \prod_{i=0}^{k-1}(q^{n-i-1}+1)$.

The number of rows of G is the number of distinct symplecta, then M= the number of symplecta of type $D_{n-k+1,1}$+ the number of symplecta of type $A_{3,2}$. So, the number of $D_{n-k+1,1}$ corresponds to the number of TI (k-1)-subspaces of V, that is: $\begin{bmatrix} n \\ k-1 \end{bmatrix}_q \prod_{i=0}^{k-2}(q^{n-i-1}+1)$ and the number of $A_{3,2}$ corresponds to the number of TI (k+2)-subspaces of V that is: $\begin{bmatrix} n \\ k+2 \end{bmatrix}_q \prod_{i=0}^{k+1}(q^{n-i-1}+1)$. Thus

$$M=\begin{bmatrix} n \\ k-1 \end{bmatrix}_q \prod_{i=0}^{k-2}(q^{n-i-1}+1)+\begin{bmatrix} n \\ k+2 \end{bmatrix}_q \prod_{i=0}^{k+1}(q^{n-i-1}+1)$$

The number of points in the symplecton of type $D_{n-k+1,1}$ is the weight w_1, thus by Theorem 4.1:

$$w_1=|\Omega^+(2(n-k+1), q)|= 2(q+1)(q^2+1)\ldots(q^{n-k+1}-1),$$

and w_2 is the number of points of symplecta of type $A_{3,2}$, that is the number of k-spaces in a (k+2)-space Then by Theorem 4.3:

$$w_2=\begin{bmatrix} k+2 \\ k \end{bmatrix}_q \prod_{i=0}^{k-1}(q^{k-i+1}+1).$$

Two rows of G have 1 in the j^{th} column if the points p_j is incident with both symplecta. Since, by Proposition 3.2, two symplecta intersect in a projective plane, a point or disjoint, it follows that the corresponding two rows differ in at least $|S_1|+|S_2|-2|S_1\cap S_2|$ positions. The least of these numbers is when the two symplecta intersect in a projective plane, it follows that the distance is:

$$d=2\min\{w_1, w_2\}-2\max|S_1\cap S_2|,$$

that is:

$$d=2(q^2+1)(q^3-1)/(q-1)-2\begin{bmatrix} k+1 \\ k \end{bmatrix}_q \prod_{i=0}^{k-1}(q^{k-i}+1). \quad \square$$

References

[1] Agrell Erik, Alexander Vardy and Kenneth Zeger, "Constant-Weight Code Bounds from Spherical Code Bounds" ISIT2000, Sorrento, Italy, June 25-30, 2000.

[2] Agrell Erik, Alexander Vardy and Kenneth Zeger, "Tables of binary block codes" Available online at www.chl.chalmers.se~agrel.

[3] Agrell Erik, Alexander Vardy and Kenneth Zeger, "Upper bounds for Constant-Weight Code" IEEE Trans. Inform. Theory, Vol. 46, pp. 2373-2395, Nov. 2000.

[4] Brouwer A. E., Cohen A. and Neumair A., "Distance regular graphs" 1986 manuscript.

[5] Cameron P.J., "Projective and Polar Spaces" volume 13 of QMW Maths Notes. Queen Mary and Westfield College, University of London, 1992.

[6] De Clerck F. and Van Maldeghem H., *Ovoids and spreads of polar spaces and Generalized Polygons*. Intensive Course on Galois Geometry and Generalized Polygons, (1985).

[7] El-Atrash M., "Constant-Weight Codes using Half-spin Geometry $D_{5,5}(q)$" . Journal of Al-Aqsa Universiy, 2002 (Preprint).

[8] Hoffman D. G., "Coding theory" II. Series, QA268.C69 1992.

[9] Thas J.A., "Old and new results results on spreads and ovoids of finite classical polar spaces" Ann.Discrete Math., 1992 52 pp.529-544.

[10] Zayda, Abdelsalam., "On Properties of point-line geometry of type $D_{n,k}(F)$" (To appear), Journal of Islamic University, 2003