Constant-weight codes using half-spin geometry $d_{5,5}(Q)$

Mohammed El-Atrash*

ملخص البحث

نولد في هذا البحث بعض مجموعات الترااميز غير الخطيـــة الثنائيـــة ذات الوزن الثابت و ذلك باستخدام الهندسة النصف-مغزلية $D_{5,5}(q)$.

Abstract

In This paper we generate few families of non-linear binary constant-weight codes using half-spin geometry $D_{5,5}(q)$. The ideas used here are the same ideas like those applied to the geometry $D_{6,6}(q)$.

Key words: Half-spin geometry, Lie incidence geometries, Constant-weight codes

AMS MSC 2000: Primary 51E30, Secondary 05B30, 94B9

*ASSOCIATE PROFESSOR - Math. Department -College of Science -Islamic University of Gaza - Gaza, Palestine

4. Introduction

Error-correcting codes have emerged as indispensable technique in modern telecommunication and information storage systems. The original ideas were developed in the early fifties of the last century by Hamming, Golay and others, mainly motivated and inspired by the fundamental and revolutionary work of Shannon in the early sixties, some of the fundamental codes were discovered such as BCH and RS codes, see [10].

Recently, Many authors have studied a certain type of codes called constant-weight codes, tables of upper and lower bounds were constructed for the sizes of a given minimal distances and a given length, see [4], [5], [6], [7].

Many papers have dealt with the subject from its algebraic point of view. This paper is one to use geometric means to define some good binary nonlinear codes. Finite geometries are considered as the raw material to construct good codes as professor Ernest Shult convinced me when I have started my geometry work under his supervision in order to get my Ph.D. degree

Here, we apply these geometric ideas to get some binary constant-weight codes. Since there are many geometries that can be used to derive such codes, this paper is to be considered the first amongst a series of papers to utilize these geometric ideas.

This paper is self-contained. For more information about the half-spin geometries see Shult [3].

5. Basic geometric definitions

Given a set I, *a* ***geometry*** Γ over I is an ordered triple $\Gamma = (X, *, D)$, where X is a set, D is a partition $\{X_i\}_{i \in I}$ of X indexed by I, X_i are called components, and $*$ is a symmetric and reflexive relation on X called incidence relation such that:

$x * y$ implies that either x and y belong to distinct components of the partition of X or $x = y$.

Elements of X are called ***objects*** of the geometry, and the objects within one component X_i of the partition are called ***objects of type*** *i*. The subscripts, which index the components, are called ***types***. The obvious mapping $\tau : X \rightarrow I$ which takes each object to the index of the component of the partition containing it is called the ***type map*** τ.

A ***point-line geometry*** (P, L) is simply a geometry for which $|I| = 2$, one of the two types is called ***points***; in this notation the points are the members of P, and the other type is called ***lines***. Lines are the members of L. In this paper we will not be concerned about geometries that contains lines that are incident with the same set of points, therefore, without loss of generality we may consider incidence as containment i.e., $p \in$ P and $l \in$ L, then $p * l$ if and only if $p \in l$. In a point-line geometry (P, L), we say that two points of P are *collinear* if and only if they are incident with a common line (we use the symbol ~ to denote collinearity).

The symbol $x^{\perp}$ means the set of all points collinear with x, including x itself. ***A partial linear space*** is a 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.

*A **subspace*** of a point-line geometry $\Gamma = (P, L)$ 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 $X \subset P$.

The ***singular rank*** of a space Γ is the maximal number n (possibly ∞) for which there exists a chain of distinct subspaces $\{X_i\}$

$$\varnothing = X_{-1} \subset X_0 \subset X_1 \subset \ldots \subset X_n ,$$

such that X_i is singular for each i, and $X_i \neq X_j$, $i \neq j$.

In a point-line geometry $\Gamma = (P, L)$, ***a path of length n*** is a sequence of $n + 1$ points; $x_0, x_1, \ldots, x_n$ 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 $d_\Gamma(x, y)$. The distance function d_Γ satisfies the following metric properties:

$$d_\Gamma : P \times P \rightarrow \{0\} \cup N \cup \{\infty\}$$

(*i*) $d_\Gamma(x, y) = 0$ if and only if $x = y$.
(*ii*) $d_\Gamma(x, y) = d_\Gamma(y, x)$
(*iii*) $d_\Gamma(x, y) + d_\Gamma(y, z) \geq d_\Gamma(x, z)$ for all $x, y, z \in P$.

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 any two points of X.

A ***geometric hyperplane*** of a geometry Γ is a subspace H with the property that $H \neq$ P and each line l of Γ, l intersects H nontrivially.

6. Some basic spaces

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 [1] 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, either $|p^{\perp} \cap l| = 1$ 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.

We write ***Rad***(Γ) for the set $\{ p : p^{\perp} =$ P$\}$, and call it the radical of Γ. A polar space Γ = (P, L) is said to be ***non-degenerate*** if and only if Rad(Γ) = $\varnothing$.

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 one 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 $l_1 \cap l_2 \neq \varnothing$, 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 $\Gamma = (P, L)$ 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; $l^{\perp}$ is 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 a parapolar space Γ, 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.

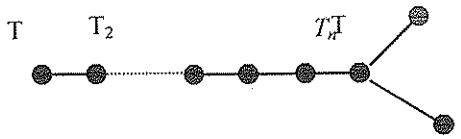
7. Definition of the half-spin geometry $D_{n,n}(F)$

Let B be a non-degenerate symmetric hyperbolic bilinear form on a vector space V of dimension $2n$ over a finite field F of order q. Define the polar space of type $\Omega^{+}_{n}(q)$ as follows: Let T_i be the set of all totally isotropic (TI) i-dimensional subspaces of V, $1 \leq i \leq n-2$. Let T_n be the class that consists of all maximal TI subspaces of dimension n. T_n is partitioned into two classes denoted by M_1 and M_2 subject to the following rule:

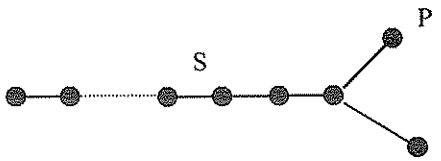
Two maximal TI subspaces m_1 and m_2 of V belong to the same class if and only if the dimension of $m_1 \cap m_2$ has the same parity as n.

i.e., if n is odd then m_1, m_2 belong to the same class iff $m_1 \cap m_2$ is of dimension 1, 3, 5, ..., n, and if n is even then m_1, m_2 belong to the same class iff $m_1 \cap m_2$ is of dimension 0, 2, 4, ..., n .

Let (P, L) be the geometry whose set of points is one of the classes say $P = M_1$ and the set of lines is the set $L = T_{n-2}$. A point $m_1 \in M_1$ is incident with a line $A \in T_{n-2}$ if and only if $m_1 \supseteq A$. The geometry $\mathbb{D}_{n,n}(\mathbb{F})$ is called the *half-spin geometry* $\mathbb{D}_{n,n}(\mathbb{F})$. If the order of F is q then we write $\mathbb{D}_{n,n}(q)$.

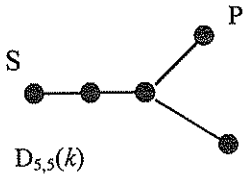


In this work we are concerned only with the half-spin geometry $\mathbb{D}_{5,5}(q)$;



Here we summarize the construction of $\mathbb{D}_{5,5}(q)$.

We have a symmetric hyperbolic bilinear form B on a vector space of dimension 10 over a finite field $F = GF(q)$. The classes M_1, M_2 consist of maximal TI 5-dimensional subspaces. Two TI 5-subspaces fall in the same class if their



intersection is of odd dimension. So the dimension of the intersection of $m_1 \cap m_2$ is 1, or 3 for distinct m_1, m_2. Thus, the points of $D_{5,5}(q)$ consists of one class (M_1, say) of the two classes of maximal TI 5-spaces, and whose set of lines corresponds to the set of all TI 3-spaces, where, a line l that correspond to a 3-subspace X is incident with the set of all points that corresponds to all TI 5-spaces that contain X.

TI 1-subspaces correspond to the set of all symplecta, where, a symplecton S that corresponds to a 1-subspace Y is the set of all TI 5-subspaces that contains Y.

TI 2-subspaces corresponds to projective subspaces of singular rank 3; A_3. TI 5-subspaces of the second class M_2 corresponds to projective subspaces of singular rank 4; A_4.

Let the map $\psi : P \rightarrow V$ defined above, i.e., $\psi(p)$ is the TI 5-space corresponding to the point p. We will use ψ for the rest of the varieties of the geometry; for example $\psi(l)$ is the TI 3-space corresponding to the line l, and, $\psi(S)$ is the TI 1-space corresponding to the symplecton S. The inverse map ψ^{-1} will be used for the inverse; for example $\psi^{-1}(\pi)$ is the symplecton corresponding to the TI 1-space π.

We will use the same notation $^{\perp}$ to mean two things; one to mean perpendicularity for subset of vectors with a bilinear form, second, to mean collinearity in the geometry.

8. Properties of $D_{5,5}(q)$

The following, Theorem 5.1, is one of two theorems of Cohen and Cooperstein [11] that sets up the connection between the algebraic and geometric structures. Theorem 5.1 has been modified by Brauaer et al. [13]. They stated that in conclusion (iii) of their theorem the geometries must be

quotient of half-spin geometries. The theorem characterizes all those strong parapolar spaces whose rank is $t \geq 2$ and satisfying the following property: $(x^{\perp} \cap S)$ is empty, a point, or a maximal singular subspace of S for all point-symplecton pair (x, S), x not a point of S.

5.1 Theorem [11]. *Let $r \geq 2$ and let* (P, L) *be a parapolar space with no thin lines, whose* maximal *singular subspaces have finite rank s, and whose symplecta have rank $r + 1$. Then* (P, L) *satisfies $(x^{\perp} \cap S)$ is either empty, a point, or a maximal singular subspace of S if and only if one of the following holds:*

(i) *$r = s$ and* (P, L) *is a non–degenerate polar space of rank $r+1$ with thick lines,*

(ii) *a: $r = 2$, $s \geq 3$, and for some natural number n between* 4 *and* $2s$-1, *and a division ring* D, $(P, L) \equiv A_{n,d}(D)$, *$d = n - s + 1$,*

b: $r = 2$, $s \geq 5$ and $(P, L) \equiv A_{2s-1, s}(D)/\langle\sigma\rangle$ *for some (infinite) division ring* D, *where σ is an automorphism of* $A_{2s-1, s}$ *induced by a polarity of the underlying projective space* PG($2s$-1, D) *of Witt index at most* s-5,

(iii) $r = 3$, $s \geq 4$ *and for* some *field* F, (P, L) *contains families* Σ , Π *of convex subspaces of* (P, L) *isomorphic to* $\mathbf{D_{4,1}(F)}$ *and* $\mathbf{D_{5,5}(F)}$ *respectively such that* Σ *is the system of symplecta of the parapolar space, and if* $(x, S) \in P \times \Sigma$ *with* $x \notin S$, $x^{\perp} \cap S$ *is a maximal singular subspace of* S *then* $\{x\} \cup S$ *lie in a unique member of* Π. *The incidence system of lines and planes lying on any point* x *is* $\mathbf{A_{s,2}(F)}$.

(iv) $r = 4$, $s = 5$ *and* (P, L) $\equiv \mathbf{E_{6,1}(F)}$ *for some field* F.

(v) $r = 5$, $s = 6$ *and* (P, L) $= \mathbf{E_{7,1}(F)}$ *for some field* F.

The relations between some of the varieties of this geometry mentioned below, proofs can be straight forward or can be deduced from either Theorem 5.1, or can be deduced from the properties of the underlying polar space.

5.2 Proposition [3]. *Let* (P, L) $= \mathbf{D_{5,5}(F)}$ *For any field F. Then the following hold*:

(1) Diameter of (P, L) is 2,

(2) S_1, $S_2 \in$ S then $S_1 \cap S_2$ is empty or a maximal singular subspace,

(3) $S \in$ S then S is a polar space of type $\mathbf{D_{4,1}(F)}$,

(4) If $x \in P$, $M \in A_4$, $x \notin M$ then $x^{\perp} \cap M$ is empty or a plane,

(5) If $x \in P$, $M \in A_3$, $x \notin M$ then $x^{\perp} \cap M$ is a point or a plane,

(6) M_1, $M_2 \in A_4$, $M_1 \neq M_2$ then $M_1 \cap M_2$ is empty or a line,

(7) M_1, $M_2 \in A_3$, $M_1 \neq M_2$ then $M_1 \cap M_2$ is a point or a plane,

(8) $M_1 \in A_3$, $M_2 \in A_4$, then $M_1 \cap M_2$ is empty, a point or a plane.

Proof. (for proof see [3]).

5.3Theorem [9, 12]. *The number of points of the finite classical polar spaces are given by the following formulae:*

$|W_{2n}(q)| = (q^{2n} - 1)/(q - 1)$,

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

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

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

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

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

5.4 Theorem. Let V be equipped with a bilinear form then the number of isotropic k-subspaces is the following:

$\begin{bmatrix} n \\ k \end{bmatrix}_q \prod_{i=0}^{k-1} \left(q^{n-i} + 1\right)$ in the symplectic case $W(2n, q)$.

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

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

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

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

Proof. See [13].

5.5Theorem [9, 12]. *The numbers of maximal totally singular subspaces of the finite classical polar spaces are given by the following formulae*:

$|\Sigma(W_{2n}(q))| = (q + 1)(q^2 + 1) \ldots (q^{2n} + 1)$,

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

$|\Sigma(\Omega^+(2n, q))| = 2(q + 1)(q^2 + 1) \ldots (q^n + 1)$,

$|\Sigma(\Omega^-(2n, q))| = (q^2 + 1)(q^3 + 1) \ldots (q^n + 1)$,

$|\Sigma(H^-(2n+1, q^2))| = (q^3 + 1)(q^5 + 1) \ldots (q^{n+1} + 1)$,

$|\Sigma(H^+(2n, q^2))| = (q + 1)(q^3 + 1) \ldots (q^n + 1)$.

9. Codes

For terminology of coding theory used in this section see [10].

Let F be a field and let n be a positive integer. Let $v = (x_1, x_2, \ldots, x_n)$. The ***Hamming weight*** function is defined as follows:

$w_h(v)$ = The cardinality of $\{i \in \{1, 2, 3, \ldots, n\} : x_i \neq 0\}$

= The number of non-zero coordinates x_i $(i = 1, 2, 3, \ldots, n)$

This defines a distance function as follows, for any two

vectors $u, v \in V$ we define the ***Hamming distance***

$$d_h: V \times V \rightarrow Z \quad by:$$

$$d_h(u, v) = w_h(u - v).$$

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

If $d = minimum \{d_h(u, v) \mid u, v \in C, u \neq v\}$; 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 V; 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 ***constant-weight code***. An (n, M, d, w)-code is a constant-weight (n, M, d)-code with w as the common weight of all codewords.

Remark if C is a constant-weight (n, M, d, w)-code then exchanging zeros and ones we get a constant-weight $(n, M, d, n - w)$-code.

10. Construction of the codes

In the following sections we will construct several families of non-linear binary constant-weight codes using the geometry $\Gamma = \mathbf{D}_{5,5}(q)$

Family I.

7.1 Theorem. Let $p_1, p_2, \ldots, p_d$ be the set of all points in Γ. Let $S_1, S_2, \ldots, S_r$ be the set of all symplecta in Γ. Let G = (g_{ij}) be the incidence matrix, where $g_{ij} = 1$ if the point p_j is incident with the symplecton S_i and $g_{ij} = 0$ otherwise. Then the rows of G represent a constant-weight binary (n, M, d, w) nonlinear binary constant-weight code of parameters:

$n = (q+1)(q^2+1)(q^3+1)(q^4+1)(q^5+1)$,
$M = (q^4+1)(q^5-1)/(q-1)$,
$d = 2(q^4-1)(q^3+1)/(q-1) - 2(q^4-1)/(q-1)$,
$w = (q^4-1)(q^3+1)/(q-1)$.

Proof. Since all symplecta have the same cardinality, it follows that rows of G have the same number of 1's. The weight of each row is the number of points in the corresponding symplecton that is $|\Omega^+(8, q)| = (q^4-1)(q^3+1)/(q-1)$; by Theorem 5.3.

Two rows of G have 1 in the j^{th} column if the point p_j is incident with both symplecta that corresponds to both rows, this means that the point is in the intersection of both symplecta. By Proposition 5.2, two symplecta intersect in a maximal singular subspace or disjoint, it follows that the corresponding two rows differ in $|S_1|+|S_2|$ or $|S_1|+|S_2| - 2|S_1 \cap S_2|$ positions. The least of these numbers is when the two symplecta intersect in a maximal singular subspace, it follows that $d = 2(q^4-1)(q^3+1)/(q-1) - 2(q^4-1)/(q-1)$. The number of rows of G is the number of distinct symplecta that is, by

Theorem 5.3, $M = (q^4+ 1)(q^5 - 1)/(q - 1)$. The number of columns of G is the number of distinct points, that is by Theorem 5.4, $n = (q+1)(q^2+1)(q^3+1)(q^4+1)(q^5+1)$.

Family II.

7.2 **Theorem.** Let $p_1, p_2, \ldots, p_d$ be the set of all points in Γ. Let $M_1, M_2, \ldots, M_n$ be the set of all maximal singular subspaces of type A_4 in Γ. Let $G = (g_{ij})$ be the incidence matrix, where $g_{ij} = 1$ if the point p_j is incident with the subspace M_i and $g_{ij} = 0$ otherwise. Then the rows of G represent a binary nonlinear constant-weight (n, M, d, w) code of parameters:

$n = (q+1)(q^2+1)(q^3+1)(q^4+1)(q^5+1)$,

$M = (q+1)(q^2+1)(q^3+1)(q^4+1)(q^5+1)$,

$d = 2(q^5 - 1)/(q - 1) - 2(q^2 - 1)/(q - 1)$,

$w = (q^5 - 1)/(q - 1)$.

Proof. Similar to the proof of Theorem 7.1.

Family III.

7.3 **Theorem.** Let $p_1, p_2, \ldots, p_d$ be the set of all points in Γ. Let $M_1, M_2, \ldots, M_n$ be the set of all maximal singular subspaces of type A_3 in Γ. Let $G = (g_{ij})$ be the incidence matrix, where $g_{ij} = 1$ if the point p_j is incident with the subspace M_i and $g_{ij} = 0$ otherwise. Then the rows of G represent a binary nonlinear constant-weight (n, M, d, w) code of parameters:

$w = (q^4 - 1)/(q - 1)$,

$n = (q+1)(q^2+1)(q^3+1)(q^4+1)(q^5+1)$,

$d = 2(q^4 - 1)/(q - 1) - 2(q^2 - 1)/(q - 1)$,

$M = (q^2+1)(q^3+1)(q^4+1)(q^5-1)/(q-1)$.

Proof. Similar to the proof of Theorem 7.1.

References

1. Buekenhout, F. and Shult, E.E. "On the foundation of polar geometry" Geometriae Dedicata (1974), 155-170.

2. El-Atrash, M. "Characterization of scalar product over various fields" 2001 preprint Islamic University of Gaza, Gaza, Palestine.

3. Shult, E.E., "Geometric hyperplanes of the half-spin geometries arise from embedding ", Bull. Belg. Math. Soc. 3 (1994) pp 439-454.

4. Agrell, E., Vardy, A., and Zeger, K., "Constant-Weight Code Bounds from Spherical Code Bounds" ISIT2000, Sorrento, Italy, June 25-30, 2000.

5. Agrell, E., Vardy, A., and Zeger, K., "Upper bounds for Constant-Weight Codes" IEEE Trans. Inform. Theory, Vol. 46, pp. 2373-2395, Nov. 2000.

6. Agrell, E., Vardy, A., and Zeger, K., "Tables of binary block codes" Available online at www.ch1.chalmers.se/~agrel.

7. Rains, E.M., and Sloane, N.J., "Tables of constant-weight binary codes" Available online at www.research.att.com/~njas/codes/Andw/index.

8. Cohen, A., *Handbook of incidence geometry*, 1993.

9. Thas, J., "Old and new results on spreads and ovoids of

finite classical polar spaces", Ann. Discrete Math. (1992) 52 pp. 529-544.

10. Rains, E., and Sloane, N., *Handbook of Coding Theory* Chapter on self-dual codes. To appear.

11. Cohen, A., and Coopersrein, B., "A Characterization of some geometries of Lie type", *Geometriae Dedicata* 15 1983 pp. 73-105.

12. DeClerck, F., and Maldeghem, H., *Ovoids and spreads of polar spaces and Generalized Polygons*. Intensive Course on Galois Geometry and Generalized Polygons.

13. Brouwer,A., Cohen, A., and Neumair, A., *Distance regular graphs 1986 manuscript.*