Turkish Journal of Mathematics

Volume 43 | Number 5 Article 9

1-1-2019

Extending self-orthogonal codes

ALP BASSA

NESRİN TUTAŞ

TÜBİTAK

Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2019) 43: 2177 – 2182
© TÜBİTAK
doi:10.3906/mat-1905-103

Extending self-orthogonal codes

Alp BASSA[1,*], **Nesrin TUTAŞ**[2]
[1]Department of Mathematics, Faculty of Science, Boğaziçi University, İstanbul, Turkey
[2]Department of Mathematics, Faculty of Science, Akdeniz University, Antalya, Turkey

Received: 24.05.2019 • **Accepted/Published Online:** 08.07.2019 • **Final Version:** 28.09.2019

Abstract: In this short note we give an exact count for the number of self-dual codes over a finite field $\mathbb{F}_q$ of odd characteristic containing a given self-orthogonal code. This generalizes an analogous result of MacWilliams, Sloane, and Thompson over the field $\mathbb{F}_2$ to arbitrary odd finite fields $\mathbb{F}_q$.

Key words: Symmetric bilinear forms, self-dual codes, maximal isotropic subspaces

1. Introduction

Let $\mathbb{F}_q$ denote the finite field with q elements. A linear code C of length n over $\mathbb{F}_q$ is a subspace of $\mathbb{F}_q^n$. On $\mathbb{F}_q^n$ we have the standard symmetric bilinear form $\langle \cdot, \cdot \rangle$ given by

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i,$$

for $x = (x_1, \dots, x_n), y = (y_1, \dots y_n) \in \mathbb{F}_q^n$. For a code C we define its dual $C^\perp$ by

$$C^\perp := \{x \in \mathbb{F}_q^n | \langle x, y \rangle = 0, \forall y \in C\}.$$

We call a code C self-orthogonal if $C \subseteq C^\perp$ and self-dual if $C = C^\perp$. The number of self-orthogonal codes of length n and dimension k is known; see Segre [7] for q odd and Pless [4] for q even. Moreover, over the field $\mathbb{F}_2$, MacWilliams et al. gave a count for the number of self-dual codes containing a given self-orthogonal code. Over a general finite field $\mathbb{F}_q$, Pless and Pierce [5] counted the number of self-dual codes containing a given self-orthogonal vector. In this paper we generalize these results by giving an exact count for the number of self-dual codes containing a given self-orthogonal code for an arbitrary finite field $\mathbb{F}_q$, with q odd. In the case that self-dual codes of given length do not exist over $\mathbb{F}_q$, we count the number of maximal self-orthogonal codes containing a given self-orthogonal code. We obtain the following result:

Theorem 1 *Let $\mathbb{F}_q$ be a finite field of odd characteristic. Let $C \subseteq \mathbb{F}_q^n$ be a self-orthogonal code of dimension k and length n.*

[*]Correspondence: alp.bassa@boun.edu.tr
2010 *AMS Mathematics Subject Classification:* 11E39, 11T71, 94B05

- *If n is odd then there are no self-dual codes in $\mathbb{F}_q^n$. The code C can be embedded in*

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

  maximal self-orthogonal codes of $\mathbb{F}_q^n$ (each of dimension $(n-1)/2$).

- *If n is even*
  - *if $4|n$ or $q \equiv 1 \mod 4$, then C is contained in*

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

    self-dual codes of $\mathbb{F}_q^n$ (each of dimension $n/2$),
  - *otherwise there are no self-dual codes in $\mathbb{F}_q^n$. The code C is contained in*

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

    maximal self-orthogonal codes of $\mathbb{F}_q^n$ (each of dimension $n/2-1$).

For $k=1$, we recover the result of Pless and Pierce [5] giving the number of self-dual codes containing a given self-orthogonal codeword.

Note that Bassa and Stichtenoth [2] showed using Witt's theorem that if self-dual codes over $\mathbb{F}_q$ of length n exist, then every self-orthogonal code can be extended to a self-dual code. Here we give an exact count for the number of ways this can be done. We do this using elementary calculations and the classification of different types of geometries over a finite field.

2. Bilinear forms over finite fields

We recall some basic facts about bilinear forms. For details, see [1, 6]. Let k be a field of characteristic different from 2. Let V be a finite dimensional vector space over k and

$$\langle \cdot, \cdot \rangle : V \times V \to k$$

be a symmetric bilinear form on V. The pair $(V, \langle \cdot, \cdot \rangle)$ will be called a symmetric bilinear space. By choosing a basis $B = \{e_1, e_2, \ldots, e_n\}$ for the vector space V, we can associate the matrix

$$A_B = \Big(\langle e_i, e_j \rangle\Big)_{1 \le i,j \le n}$$

to the bilinear form $\langle \cdot, \cdot \rangle$. Let $B' = \{e'_1, e'_2, \ldots, e'_n\}$ be another basis for V. Then we have

$$A_{B'} = P^T A_B P, \tag{1}$$

where P is the change of basis matrix from B' to B and P^T denotes the transpose of P. Hence, the matrix of $\langle\cdot,\cdot\rangle$ is well defined up to congruence. We define the discriminant of a $(V,\langle\cdot,\cdot\rangle)$ as the determinant of the matrix associated to $\langle\cdot,\cdot\rangle$. From (1), we see that the discriminant of $(V,\langle\cdot,\cdot\rangle)$ is uniquely determined up to multiplication by squares in $k^\times$.

Let $(V,\langle\cdot,\cdot\rangle_V)$ and $(V',\langle\cdot,\cdot\rangle_{V'})$ be two symmetric bilinear spaces. A linear transformation $\sigma : V \to V'$ is called an isometry of symmetric bilinear spaces if for all $u, v \in V$ we have

$$\langle\sigma(u),\sigma(v)\rangle_{V'} = \langle u,v\rangle_V \ .$$

Two symmetric bilinear spaces $(V,\langle\cdot,\cdot\rangle_V)$ and $(V',\langle\cdot,\cdot\rangle_{V'})$ will be called isomorphic if there exists a bijective isometry $\sigma : V \to V'$.

Let $(V,\langle\cdot,\cdot\rangle)$ be a symmetric bilinear space. Two vectors $u, v \in V$ are said to be orthogonal if $\langle u,v\rangle = 0$. For a subspace W of V, the orthogonal space $W^\perp$ is defined by

$$W^\perp := \{v \in V | \langle v,w\rangle = 0, \forall w \in W\}.$$

$(V,\langle\cdot,\cdot\rangle)$ will be called nondegenerate (regular), if $V^\perp = \{0\}$. For subspaces U, W of V we have

$$U \subseteq W \implies W^\perp \subseteq U^\perp. \tag{2}$$

If $(V,\langle\cdot,\cdot\rangle)$ is nondegenerate, it can be shown that for a subspace W

$$\dim V = \dim W + \dim W^\perp. \tag{3}$$

The subspace W of V is called totally isotropic if $\langle w_1,w_2\rangle = 0$ for all $w_1, w_2 \in W$, or equivalently, if $W \subseteq W^\perp$. If V is nondegenerate we see by Eq. (3) that for a totally isotropic subspace W we have $\dim W \leq \dim V/2$.

Next we consider the dimension of the maximal isotropic subspace of a symmetric bilinear space V. Let $(V,\langle\cdot,\cdot\rangle)$ be a nondegenerate symmetric bilinear space and U, W be totally isotropic subspaces of V with $\dim U \leq \dim W$. Then by Witt's theorem there exists a totally isotropic subspace U' containing U with $\dim U' = \dim W$. In particular, all maximal totally isotropic subspaces of $(V,\langle\cdot,\cdot\rangle)$ have the same dimension. Hence, the dimension of the maximal isotropic subspace is well defined. This dimension is given by the classification in Theorem 2 below. By (2), all isotropic subspaces containing U must be in $U^\perp$. Therefore, any maximal isotropic subspace containing U lies in $U^\perp$.

We will implicitly use the following basic result about finite fields:

Let $\mathbb{F}_q$ be a finite field with q elements of characteristic different from 2.

1. $|\mathbb{F}_q^\times/{\mathbb{F}_q^\times}^2| = 2$.
2. If $q \equiv 1 \pmod 4$, then -1 is a square in $\mathbb{F}_q$. If $q \equiv 3 \pmod 4$, then -1 is not a square in $\mathbb{F}_q$.

The classification of symmetric bilinear spaces over $\mathbb{F}_q$ up to isometry (geometries over $\mathbb{F}_q$) is well known. See [1, 6]. It can be summarized as follows

Theorem 2 *Let $\mathbb{F}_q$ be a finite field with q elements. For any dimension n, there are two nondegenerate symmetric bilinear spaces of dimension n over $\mathbb{F}_q$, up to isometry. These are determined by the discriminant (modulo squares) of the bilinear form.*

- *If n is odd, there are two distinct geometries, called TYPE I and TYPE II, characterized by whether the discriminant of the bilinear form is square or nonsquare. However, these geometries are similar; in both cases the dimensions of the maximal isotropic subspaces are $(n-1)/2$.*

- *If n is even, there are two distinct geometries. A TYPE III geometry has discriminant equal to $(-1)^{n/2}$ (modulo squares in $\mathbb{F}_q$) and the dimensions of its maximal isotropic subspaces are $n/2$. Otherwise, we have a TYPE IV geometry, and the maximal isotropic subspaces have dimension $n/2-1$.*

On $\mathbb{F}_q^n$ we have the standard bilinear form $\langle\cdot,\cdot\rangle$ given by

$$\langle x, y\rangle = \sum_{i=1}^{n} x_i y_i,$$

for $x=(x_1,\dots,x_n), y=(y_1,\dots y_n)\in\mathbb{F}_q^n$. It is nondegenerate, its matrix is the $n\times n$ identity matrix I_n, and its discriminant is 1. A code is a subspace of $\mathbb{F}_q^n$, and it is said to be self-orthogonal if it is a totally isotropic subspace of $(\mathbb{F}_q^n,\langle\cdot,\cdot\rangle)$. A self dual code of length n over $\mathbb{F}_q$ exists if $(\mathbb{F}_q^n,\langle\cdot,\cdot\rangle)$ is a geometry of TYPE III. By Theorem 2, this is equivalent to $1=(-1)^{n/2}$ modulo squares in $\mathbb{F}_q$, and hence a self-dual code over $\mathbb{F}_q$ of length n does exist if and only if $(-1)^{n/2}$ is a square in $\mathbb{F}_q$, i.e. if $4|n$ or $q\equiv 1 \mod 4$.

3. Embedding self-orthogonal codes into self-dual codes

Consider $\mathbb{F}_q^n$ with the standard bilinear form $\langle\cdot,\cdot\rangle$ on $\mathbb{F}_q$. Let C be a self-orthogonal code over $\mathbb{F}_q$ of dimension k of length n. Let $C^\perp$ be the dual code, which will have dimension $n-k$. Since C is self-orthogonal, we have $C\subseteq C^\perp$. Consider the quotient space $C^\perp/C$. It is again an $\mathbb{F}_q$ vector space of dimension $n-2k$. We have the canonical projection map $\pi: C^\perp\to C^\perp/C$. The bilinear form $\langle\cdot,\cdot\rangle$ on $\mathbb{F}_q$ induces a bilinear form on the quotient space $C^\perp/C$

$$[\cdot,\cdot]: C^\perp/C\times C^\perp/C\to\mathbb{F}_q,\quad [x+C, y+C]=\langle x,y\rangle,$$

where $x,y\in C^\perp$. It is immediate to see that $[\cdot,\cdot]$ is a well-defined bilinear form on $C^\perp/C$. Moreover, $[\cdot,\cdot]$ is nondegenerate.

Proposition 3 *Consider the canonical projection map $\pi: C^\perp\to C^\perp/C$. Using π we can associate to each subspace J of $C^\perp/C$ the subspace $\pi^{-1}(J)$ of $C^\perp$.*

(i) This gives a bijective correspondence between subspaces of $C^\perp/C$ and subspaces of $C^\perp$ containing C.

(ii) If J is a subspace of $C^\perp/C$ of dimension r, then $\pi^{-1}(J)$ is a subspace of $C^\perp$ of dimension $k+r$.

(iii) If J is a totally isotropic subspace of $C^\perp/C$, then $\pi^{-1}(J)$ is a totally isotropic subspace of $C^\perp$ (hence also of $\mathbb{F}_q^n$) containing C.

(iv) If $\mathcal{M}$ is a maximal isotropic subspace of $C^\perp/C$, then $\pi^{-1}(\mathcal{M})$ is a maximal isotropic subspace of $C^\perp$ containing C. Hence, $\pi^{-1}(\mathcal{M})$ is also a maximal isotropic subspace of $\mathbb{F}_q^n$.

(v) *The number of maximal isotropic subspaces of $C^\perp/C$ is equal to the number of maximal isotropic subspaces of $\mathbb{F}_q^n$ containing C.*

Proof (i) and (ii) follow from the isomorphism theorem. (iii) Let $\alpha, \beta \in \pi^{-1}(J)$. Then $\langle \alpha, \beta \rangle = [\alpha + C, \beta + C] = [\pi(\alpha), \pi(\beta)] = 0$, since J is a totally isotropic subspace of $C^\perp/C$. Therefore, $\pi^{-1}(J)$ is a totally isotropic subspace of $C^\perp$ (and hence also of $\mathbb{F}_q^n$) containing C. (iv) $\pi^{-1}(\mathcal{M})$ is an isotropic subspace of $\mathbb{F}_q^n$, which is maximal among the isotropic subspaces of $C^\perp$ containing C. If U is a maximal isotropic subspace of $\mathbb{F}_q^n$ containing C, then by (2), $U \subseteq C^\perp$ and hence by the maximality of $\pi^{-1}(\mathcal{M})$ we have $U = \pi^{-1}(\mathcal{M})$. Hence, $\pi^{-1}(\mathcal{M})$ is a maximal isotropic subspace of $C^\perp$ and $\mathbb{F}_q^n$ containing C. (v) follows directly from (iv). □

Let $\{e_1, ..., e_k\}$ be a basis of C and extend it to a basis $\{e_1, ..., e_{n-k}\}$ of $C^\perp$. A basis of $C^\perp/C$ is given by $\{e_{k+1} + C, ..., e_{n-k} + C\}$. Denote by

$$G = \Big([e_i + C, e_j + C]\Big)_{k+1 \le i,j \le n-k} = \Big(\langle e_i, e_j \rangle\Big)_{k+1 \le i,j \le n-k}$$

the matrix associated to the bilinear form $[\cdot,\cdot]$ on $C^\perp/C$ with respect to this basis. Our aim is to determine the type of the geometry $(C^\perp/C, [\cdot,\cdot])$. The dimension of $C^\perp/C$ is $n-2k$, and we only need to determine the discriminant of $[\cdot,\cdot]$.

Extending $\{e_1, ..., e_{n-k}\}$ to a basis $\{e_1, \ldots, e_n\}$ of $\mathbb{F}_q^n$ ($\{e_1, \ldots, e_k\}$ is a basis for C, and $\{e_1, \ldots, e_{n-k}\}$ is a basis for $C^\perp$). The matrix corresponding to the bilinear form $\langle \cdot,\cdot \rangle$ on $\mathbb{F}_q^n$ with respect to this basis is given by

$$M = \begin{bmatrix} 0_{k\times k} & 0_{k\times(n-2k)} & D_{k\times k} \\ 0_{(n-2k)\times k} & G_{(n-2k)\times(n-2k)} & E_{(n-2k)\times k} \\ D^T_{k\times k} & E^T_{k\times(n-2k)} & Z_{k\times k} \end{bmatrix}.$$

Here $G = G_{(n-2k)\times(n-2k)}$ is the matrix corresponding to the bilinear form $[\cdot,\cdot]$ on $C^\perp/C$, and our aim is to determine the determinant of G.

M is not necessarily the identity matrix since we have not chosen the standard basis for $\mathbb{F}_q^n$, but a basis coming from a basis for C and $C^\perp$. The matrix M is, however, congruent to the identity matrix and its determinant is a square in $\mathbb{F}_q$, say α. To determine the determinant of G we use column operations to turn M into block diagonal form. More precisely, for $1 \le i \le k$ we interchange column i and column $n-k+i$. These k column operations will multiply the determinant by $(-1)^k$ and result in the matrix M' with determinant $(-1)^k \cdot \alpha$.

$$M \xrightarrow{\text{column operations}} \begin{bmatrix} D_{k\times k} & 0_{k\times(n-2k)} & 0_{k\times k} \\ E_{(n-2k)\times k} & G_{(n-2k)\times(n-2k)} & 0_{(n-2k)\times k} \\ Z_{k\times k} & E^T_{k\times(n-2k)} & D^T_{k\times k} \end{bmatrix} = M'$$

Determinants of block diagonal matrices are easily calculated:

$$\det M' = \det G \cdot (\det D)^2 = (-1)^k \cdot \det M = (-1)^k \cdot \alpha,$$

with $\alpha \in \mathbb{F}_q^{\times 2}$. We obtain the following:

Proposition 4 *$(C^{\perp}/C, [\cdot,\cdot])$ is a symmetric bilinear space of dimension $n-2k$ and discriminant $(-1)^k \in \mathbb{F}_q^{\times}/{\mathbb{F}_q^{\times}}^2$.*

The number of maximal isotropic subspaces for geometries of each type was given by Segre [7]:

Proposition 5 (Segre) *Let $(V, \langle\cdot,\cdot\rangle)$ be a symmetric bilinear form over $\mathbb{F}_q$ of dimension r, and the discriminant d, where q is odd.*

- *If r is odd, then $(V, \langle\cdot,\cdot\rangle)$ is of TYPE I or TYPE II, and the maximal isotropic subspace of V has dimension $\nu = (r-1)/2$. The total number of maximal isotropic subspaces is given by*

$$\sigma_{r,\nu} = \prod_{i=1}^{\nu}(q^i+1).$$

- *If r is even and $d = (-1)^{r/2}$ modulo squares in $\mathbb{F}_q^{\times}$, then $(V, \langle\cdot,\cdot\rangle)$ is of TYPE III, and the maximal isotropic subspace of V has dimension $\nu = r/2$. The total number of maximal isotropic subspaces is given by*

$$\sigma_{r,\nu} = 2 \cdot \prod_{i=1}^{\nu-1}(q^i+1).$$

- *If r is even and $d \neq (-1)^{r/2}$ modulo squares in $\mathbb{F}_q^{\times}$, then $(V, \langle\cdot,\cdot\rangle)$ is of TYPE IV, and a maximal isotropic subspace of V has dimension $\nu = n/2-1$. The total number of maximal isotropic subspaces is given by*

$$\sigma_{r,\nu} = \prod_{i=2}^{\nu+1}(q^i+1).$$

Combining Propositions 3, 4, and 5, we obtain Theorem 1.

References

[1] Artin E. Geometric Algebra. New York, NY, USA: Interscience Publishers Inc., 1957.

[2] Bassa A, Stichtenoth H. Self-dual codes better than the Gilbert–Varshamov bound. Designs, Codes and Cryptography 2019; 87: 173-182.

[3] MacWilliams FJ, Sloane NJA, Thompson JG. Good self dual codes exist. Discrete Mathematics 1972; 3: 153-162.

[4] Pless V. The number of isotropic subspaces in a finite geometry. Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali 1965; 39: 418-421.

[5] Pless V, Pierce JN. Self-dual codes over GF(q) satisfy a modified Varshamov-Gilbert bound. Information and Control 1973; 23: 35-40.

[6] Scharlau W. Quadratic and Hermitian Forms. Berlin, Germany: Springer-Verlag, 1985.

[7] Segre B. Le geometrie di Galois. Annali di Matematica Pura ed Applicata 1959; 48 (4): 1-96 (in Italian).