OUR HERITAGE
ISSN: 0474-9030 Vol-68, Special Issue-6
Impact Factor (2020) - 6.8
Special Issue on *"Importance of Mathematics Education"*

A Note on extended binary Schubert Code

Mahesh S Wavare1*, Dr. Suryakant M Jogdand[2], Dr. Arunkumar R Patil[3]
1Rajarshi Shahu Mahavidyalaya,Latur,(Autonomous) maheshwavare@gail.com
2 S.S. S. G. M. College,Loha, smjog12@gmail.com
3 S. G. G. S. Institute of Engg &Tech,Nanded arun.iitb@gmail.com
*Presenting author

Abstract:

Linear error correcting codes associated to higher dimensional algebraic varieties defined over finite fields have been topical interest. For example codes associated to Hermitian varieties, Grassmanian varieties, Schubert varieties and Flag varieties have been studied quite extensively .The codes associated to these types of varieties is the central interest. Codes associated with Schubert varieties in $G(2,5)$ over F_2have been studied in [14] .The corresponding extended binary Schubert code is denoted by $\bar{\Omega}_{19}$ and its generator matrix is given in [1] having order 5×19.
In this paper we have discussed the properties of extended binary Schubert Code $\bar{\Omega}_{19}$

1. Introduction:

In [13], Victor Wei initiated the idea of weight hierarchy of a linear code, aggravated by application in type II wire-tap channel in cryptography. Wei introduced the r-th generalized Hamming weight of a linear code as the minimum support weight of any of its *r*-dimensional subcode. For a class of Algebraic-geometric codes the generalized Hamming weights were investigated by a number of researchers such as Tsfasmann-Vladut [12], 1 Nogin [8], Ghorpade-Lachaud [1], Ghorpade-Tsfasman [2], Hirshfeld-Tsfasman-Vladut [7], Ghorpade-Patil-Pillai [3]. Generalized Hamming weights proved to be of enormous applications in coding theory to study the structure of a code. It is therefore natural to consider an extension of the notion of generalized weights-the generalized spectra of linear codes.

The problem of determining the generalized spectra of a linear $[n, k]_q$ code is first studied by Klove in [4] and [5]. In [4], he gave a MacWilliams identity for the support weight distribution of linear codes called the generalized MacWilliams identity. In [5], he determined the weight enumerator polynomial (also called support weight distribution function) for irreducible cyclic codes.

In [3], the problem of determining generalized spectrum for another class of linear codes arising from higher dimensional projective varieties namely Grassmannians varieties is studied.

The generalized spectrum of code associated with Schubert sub varieties of Grassmannians $G(2, 5)$ over F_2 is determined by [14]. In this paper the corresponding binary Schubert code is denoted by Ω_{19} is defined whose generator matrix is found in [14] having order 5×19.In this paper we have discussed all the properties of this binary Schubert code and found extended binary Schubert Code $\bar{\Omega}_{19}$.

2. Linear Codes:

2.1 Basic definitions: Let F_q denote the finite field with q elements, $q = p^h$, p a prime and h a natural number .We denote F_q^n as the *n*-dimensional vector space over F_q. For any $x \in F_q^n$, the support of (x), is the nonzero entries in $x = (x_1, x_2,..., x_n)$. The support weight (or Hamming norm) of x is defined by, $\|x\| = |\sup p(x)|$.

More generally, if W is a subspace of F_q^n, the support of W, Supp (W) is the set of positions where not all the vectors in W are zero and the support weight (or Hamming norm) of W is defined by,

OUR HERITAGE
ISSN: 0474-9030 Vol-68, Special Issue-6
Impact Factor (2020) - 6.8
Special Issue on *"Importance of Mathematics Education"*

$$\|W\| = |\text{supp}(W)|$$

A linear $[n,k]_q$-code is a *k*-dimensional subspace of F_q^n. The parameters *n* and *k* are referred to as the length and dimension of the corresponding code. The minimum distance d = d(C) of C is defined by

$$d = d(C) = \min\{\|x\| : x \in C, x \neq 0\}$$

More generally, given any positive integer *r*, the r^{th} higher weight $d_r = d_r(C)$ is defined by

$$d_r = d_r(C) = \min\{\|D\| : D \text{ is a subspace of } C \text{ with } \dim D = r\}$$

Note that $d_1(C) = d(C)$. It also follows that $d_i \leq d_j$ when $i \leq j$ and that $d_k = |\sup p(C)|$,where *k* is dimension of code C. Thus we have $1 \leq d_1 = d < d_2 < ... < d_{k-1} < d_k = n$. The first weight d_1 is equal to the minimum distance and the last weight is equal to the length of the code.

An $[n,k]_q$ -code is said to be nondegenerate if it is not contained in a coordinate hyperplane of F_q^n. Two $[n,k]_q$ -codes are said to be equivalent if one can be obtained from another by permuting coordinates and multiplying them by nonzero elements of F_q. It is clear that this gives a natural equivalence relation on the set of $[n,k]_q$ -codes.

The (usual) spectrum (or weight distribution) of a code $C \subseteq F_q^n$ is the sequence $\{A_o, A_1, ..., A_n\}$ defined by $A_i = A_i(C) = |\{c \in C : \|c\| \neq 0\}|$.

More generally, the r^{th} higher weight spectrum (or r^{th} support weight distribution) of a code C is the sequence $\{A_0^r, A_1^r, ...A_n^r,\}$ defined by

$$A_i^r = |\{D \subseteq C : \dim D = r, \|D\| = i\}| \qquad (2.1)$$

This naturally allows us to define rth support weight distribution function (or r^{th} weight enumerator) as

$$A^r(Z) = A_0^r + A_r^1 Z + ... + A_r^n Z^n \qquad (2.2)$$

Hence for each $0 \leq r \leq k$, we have a weight enumerator. We can also define the rth higher weight as $d_r(C) = \min\{i : A_i^r \neq 0\}$.

Note that $A^0(Z) = 1$. Also note that if $\bar{x} \in F_q^n$, then

$$\|x\| = \|\{\bar{x}\}\| = \|\{\lambda \bar{x} : \lambda \in F_q\}\|.$$

Lemma 2.1 If C is a code with dimension k over F_2 then for Z = 1

$$A^r(1) = \begin{bmatrix} k \\ r \end{bmatrix}_2 \qquad (2.3)$$

Where $\begin{bmatrix} k \\ r \end{bmatrix}_2 = \frac{(2^k-1)(2^k-2)..(2^k-2^{r-1})}{(2^r-1)(2^r-2)..(2^r-2^{r-1})}$,which is the number of subspaces of dimension r in *a K* dimensional space.

2.2 Self Orthogonal Codes:

The standard inner product on F_q^n is defined by $\langle x, y \rangle := \sum_{i=1}^n x_i y_i$

OUR HERITAGE
ISSN: 0474-9030 Vol-68, Special Issue-6
Impact Factor (2020) - 6.8
Special Issue on *"Importance of Mathematics Education"*

Definition 2.2.1 The Dual of a code $C \subseteq F_q^n$ is the code

$C^{\perp} := \{x \in F_q^n : \langle x, c \rangle = 0 \text{ for all } c \in F_q^n\}$ and code code C is called self orthogonal if $C^{\perp}$ is subset of C.

Let $B^r(Z)$ be the r^{th} support weight distribution function of the dual cod $C^{\perp}$. In [4] Klove gave the MacWilliams identity for the generalized spectrum of code C and its dual,

Theorem 2.2.1 (Generalized MacWilliams Identity) For all $m \geq 0$ we have

$$\sum_{r=0}^{m} [m]_r B^r(Z) = q^{-mk}\left[1+(q^m-1)Z\right]^n \left\{\sum_{r=0}^{m} [m]_r A^r\left(\frac{1-Z}{1+(q^m-1)Z}\right)\right\},$$

where $[m]_r = (q^m-1)(q^m-q)(q^m-q^2)..(q^m-q^{r-1})$.

The number $[m]_r$ is known as the number of the ordered linear independent *r*-elements in the *m*-dimensional space.

For *r* = 1, we can write the MacWilliams identity for usual spectrum in the following theorem.

Theorem 2.2.3 1 + (q-1+$(q-1)B^1(Z) = q^{-k}(1+(q-1)Z)^n\left\{1+(q-1)A^1\left(\frac{1-Z}{1+(q-1)Z}\right)\right\}$

3. Projective Systems : An alternative way to describe codes is via the language of projective systems introduced in [Q_{12}]. Let P^{k-1} be a projective space of dimension k-1over F_q. $A[n,k]_q$ -projective system is a (multi)set X of *n* points in the projective space P^{k-1} over Fq . We call X nondegenerate if these *n* points are not contained in any hyper plane of P^{k-1}. Two $[n,k]_q$ -projective systems are said to be equivalent if one can be obtained from another by a projective transformation. For any positive integer *r*, the r^{th} higher weight of a projective system X is defined by

$$d_r = d_r(X) = n - \max\{|X \cap \prod| : \prod \text{ is a subspace of } P^{k-1} \text{ of co dim ension } r\}$$

The generalized spectrum of a projective system X is defined by,

$$A_i^r = A_i^r(X) = \left|\{\prod \subseteq P^{k-1} : |X \cap \prod| = n-i, co \dim \prod = r\}\right|$$

for all *i* = 1, 2, ..., n, *r* = 1, 2, ... It can be proved that $A_i^r = A_i^r(C) = A_i^r(X)$.

For any $[n,k]_q$ -linear code C, one can construct corresponding $[n,k]_q$ -projective system in the following way: Consider coordinate forms $x_i : C \to F_q$ such that

$$x_i : (v_1,...,v_n) \mapsto v_i$$

These forms can be considered as *n* points of the space *C** of linear functions on *C* (the dual linear space). If *C* is nondegenerate, that is, all forms x_i are nonzero as functions on *C*, then they define *n* points in $P^{k-1} = p(C^*)$, or a projective system.

A subcode $D \subset C$ of dimension *r* correspond to the set of elements of *C** vanishing on D, that is, to the subspace $D^* \subset C^*$ of codimension *r* and, therefore, to a subspace of codimension *r* in P^{k-1}. The weight of a subcode *D* equals to the number of coordinate forms not vanishing on it, that is, the number of points of X not lying on this subspace of codimension *r*.

On the other hand, now we show how one can construct a linear code for a nondegenerate projective system. Given a projective system $X = \{P_1, P_1,..., P_n,\} \subset P^{k-1} = P(V)$, we lift it to a system

OUR HERITAGE
ISSN: 0474-9030 Vol-68, Special Issue-6
Impact Factor (2020) - 6.8
Special Issue on *"Importance of Mathematics Education"*

$\{y_1, y_2,..., y_n\}$ of vectors in V . Any y_i defines a mapping $V^* \to F_q$, and the set $\{y_1, y_2,..., y_n\}$ defines the mapping $V^* \to F_q^n$, given by $(v_1, v_2,...v_n,) \mapsto (y_1(v), y_2(v),..., y_n(v))$ whose image is some linear code. Moreover it is an $[n,k]_q$ -code if the projective system is nondegenerate.

The above correlation provides the proof for the following theorem. (see12)

Theorem 3.1 There is a one-to-one correspondence between the set of the equivalence classes of nondegenerate $[n,k]_q$ -projective systems and the set of the equivalence classes of nondegenerate linear $[n,k]_q$ -codes. This correspondence preserves the parameters *n, k* and the higher weights $d-1, d_2,..., d_k$.

The above correspondence in terms of generator matrix can be viewed as follows: Let G is a generator matrix for a $[n,k]_q$ -linear code *C*, and let $g_1, g_2, \ldots, g_n \in F_q^k$ be the columns of *G*. Suppose that none of the g_i's is the zero vector. then each g_i determines a point $[g_i]$ in the projective space $P^{k-1} = P(F_q^k)$. If these g_i are pairwise independent, then $X := \{|g_1|, |g_2|,..., |g_n|,\}$ is a set of *n* points in P^{k-1} . This will be the corresponding projective system. Thus the *n* columns of *G* determines a projective system X. Vice versa, If X is a projective system, then a generator matrix for *C* is the $k \times n$ matrix whose columns are the representatives of points in projective system X.

3.2 Codes from Schubert Varieties :

Ghorpade and Lachaud in [1] proposed the generalization of Grassmann codes as Schubert codes. The Schubert codes are indexed by the elements of the set

$$I(l,m) := \{\alpha = (\alpha_1, \alpha_2,..., \alpha_l) \in Z : 1 \le \alpha_1 < ... < \alpha_l \le m\},$$

Given any $\alpha \in I(l,m)$, the corresponding Schubert code is denoted by $C_\alpha \in (l,m)$, and it is the code obtained from the projective system defined by the Schubert variety Ω_α in *G(l, m)* with a nondegenerate embedding induced by the Plücker embedding. We define Ω_α as

$$\Omega_\alpha = \{W \in G(l,m) : \dim(W \cap A_{\alpha i}) \ge i \ \ for i = 1,2,...,l\},$$

where A_j denotes the span of the first *j* vectors in a fixed basis of V, for $1 \le j \le m$. Ghorpade and Tsfasman in [2], determined the length n_α and dimension k_α of $C_\alpha(l,m)$. It was conjectured by Ghorpade in [1], that

$$d(C_\alpha(l,m)) = q^{\delta\alpha} \qquad (3.4)$$

where $\delta_\alpha := \sum_{i=1}^{l} (\alpha_i - i) = \alpha_1 + \alpha_2 + ... + \alpha_l - \frac{l(l+1)}{2}$ .The complete weight hierarchy and second support weight distribution of codes associated with all Schubert subvarieties of *G(2, 4)* is known due to Patil ([9]).

4 Codes associated with Schubert varieties in *G(2, 4)* over F_2 :

Let *I(2, 4)* be an indexing set defined by,

I(2,4) : = {(1,2), (1,3), (1,4), (2,3), (2,4), (3,4)}

Now by definition given any $\alpha \in I(l,m)$, the Schubert variety is defined by,

$$\Omega_\alpha := \{P \in G(l,m) : p_\beta = 0 \ \ \forall \ \beta \ne \alpha\}$$

We consider Schubert varieties for each above and the codes associated with them.

OUR HERITAGE
ISSN: 0474-9030 Vol-68, Special Issue-6
Impact Factor (2020) - 6.8
Special Issue on *"Importance of Mathematics Education"*

The projective system consists of F_2-rational points of $\Omega_{(2,4)}$. The number of rational points on $\Omega_{(2,4)}$ is given by,

$$\begin{aligned} n &= \sum_{\beta \le \alpha} q^{\delta\beta} \\ &= 2^{1+2-3} + 2^{1+3-3} + 2^{1+4-3} + 2^{2+3-3} + 2^{2+4-3} \\ &= 1+2+4+4+8 \\ &= 19 \end{aligned}$$

We have considered the 5×19 matrix as a generator matrix for Schubert code which is defined here

4.1 Definition

Extended Binary Schubert Code $\overline{\Omega}_{19}$

Let G be the 5×19 matrix given by

$$G = \begin{bmatrix} 1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,1\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,0\,0\,1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,0\,0\,1 \\ 0\,0\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,1\,0\,0\,1\,0\,1\,0 \\ 0\,0\,0\,0\,1\,1\,1\,0\,0\,1\,0\,1\,0\,0\,1\,1\,1\,0\,0 \end{bmatrix}$$

i.e $G = [I_5|X]$ Where $X = \begin{bmatrix} 0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,0\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0 \\ 0\,1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,0\,0\,1 \\ 1\,0\,1\,0\,1\,0\,1\,1\,0\,0\,1\,0\,1\,0 \\ 1\,1\,0\,0\,1\,0\,1\,0\,0\,1\,1\,1\,0\,0 \end{bmatrix}$ is 5×14 matrix

The binary linear code whose generator matrix is G is called extended binary Schubert code and it is denoted by $\overline{\Omega_{19}}$.

4.2 Properties of extended binary Schubert code

In this section we will discuss some of its properties

Proposition 4.2.1

Let $\overline{\Omega}_{19}$ be the extended binary code generated by matrix G which is defined above then following properties holds for the corresponding code

i) The length of $\overline{\Omega}_{19}$ is 19.

ii)The dimension of $\overline{\Omega}_{19}$ is 5

iii)The parity check matrix for $\overline{\Omega}_{19}$ is the matrix 14×19 matrix ,$H = [X^t|I_{14}]$

iv)$\overline{\Omega}_{19}$ is self orthogonal linear code.

v) The weight of every codeword is multiple of 2

vi) The code $\overline{\Omega}_{19}$ has no codeword of weight 2

vii) The linear code $\overline{\Omega}_{19}$ is exactly three error correcting code .

Proof:

i) By looking at generator matrix of $\overline{\Omega}_{19}$ length is clear

ii) Dimension of $\overline{\Omega}_{19}$ is 5 since Generator matrix of $\overline{\Omega}_{19}$ consist of I_5

iii)By applying algorithm of finding parity check matrix of $\overline{\Omega}_{19}$ we get desired result

iv)In the generator matrix every row vector is mutually orthogonal to other so $\overline{\Omega}_{19}$ self orthogonal code

v) In the basis weight of every codeword is even so weight of every codeword in this code $\overline{\Omega}_{19}$ is divisible by 2

vi)since minimum weight of every codeword in basis is 8 so there do not exist a codeword of weight 2

vii)Distance of this code 8 so it is an exactly 3-error correcting code

hence proved

5. Conclusion

In this article we defined extended binary Schubert code $\overline{\Omega}_{19}$ of length 19 ,dimension 5 and distance 8.i.e $\overline{\Omega}_{19}$ is a binary [19,5,8] linear code some properties of it are discussed

6. References :

[1] Ghorpade, S.R., Lachaud, G., Higher weights of Grassmann codes, Coding Theory, Cryptography and Related Areas (J. Buchmann, T. Hoeholdt, H. Stictenoth, and H. Tapia - Resillas, Eds.) Springer-Verlag, Heidelberg, G Germany , 120-131, (2000).

[2] Ghorpade, S.R., Tsfasman, M.A., Schubert varieties, linear codes and enumerative combinatorics, Finite Fields and Their Applications. vol. 11, No.4, pp.684- 699,(2005).

[3] Ghorpade, S.R., Patil A. R., Pillai H. Decomposable subspaces, linear sections of Grassmann varieties, and higher weights of Grassmann codes , Finite Fields and Their Applications vol. 15, No. 1, pp.54-68,(2009).

[4] Klove, Torleiv, Support weight distribution of linear codes, Discrete Mathematics 106/107, 311-316, (1992).

[5] Klove, Torleiv, The weight distribution of linear codes over GF(q^l) having generator matrix over GF(q*), Discrete Mathematics 23, 159-168, (1978).

[6] Hirschfeld, J.W.P., Tsfasman, M.A., Vladut', S.G., The weight hierarchy of higherdimensional Hermitian codes , IEEE Trans. Inform. Theory 40, 275-278, (1994).

[7] J.P. Hansen, T. Johnsen, K. Ranestad, Schubert unions in Grassmann varieties, Finite Fields Appl.13, 738750 (2007)

[8] Nogin, D.Yu., Codes associated to Grassmannians, Arithmetic, Geometry and Coding Theory R. Pellikan, M. Perret, S.G. Vladut'. Eds., 145-154,Walter de Gruyter, Berlin/ New York,(1996).

[9] Patil, A.R., Generalized Spectrum of Grassmann Codes, Proceedings of Asian Mathematical Conference 2005 (AMC 2005) held at NUS, Singapore.

[10] Ryan, C. T. An application of Grassmannian varieties to coding theory, Congr. Numer. 57, 257-271, (1987).

[11] Ryan, C. T. Projective codes based on Grassmann varieties , Congr. Numer. 57, 273-279, (1987).

[12] Tsfasman, M.A., Vladut', S.G. Algebraic Geometric Codes, Kluwer, Amsterdam, (1991).

[13] Wei, V. K. Generalized Hamming weights for linear codes, IEEE Trans. Inform. Theory 37 , 1412-1418, (1991).

[14] Mahesh S. Wavare,Codes associated to Schubert varieties G(2,5) over F_2 New Trends in Mathematical Sciences , Vol.7(Issue 1), 2019r, Pg. no. 71-78. DOI: 10.20852/ntmsci.2019.343