International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 11 Issue 4, April-2022, Impact Factor: 7.957

Binary Grassmann Matrix Product Codes

Dattatraya Sadashivrao Mangnale

Asst. Teacher Mahatma Gandhi Secondary and Higher Secondary School,
Mudkhed (Jn.) Dist: Nanded (MH) India

Abstract

In this paper we construct the matrix product code using generator matrix of Grassmann codes associated with projective Grassmann variety over a binary field. We determine the parameters length, dimension, minimum distance, and size of these codes.

Introduction

Matrix product codes over finite field F_q were introduced by Blackmore and Norton[1] as a generalization of certain well known construction of linear codes such as Plotkin's construction, the ternary construction, and etc. Later on the decoding algorithms of these codes were studied by Hernando, lally, and Ruano [5]. Ozbudak and H. Stichtenoth [8].

The study of Grassmann codes was initiated by Ryan and Ryan [10] and later ex-tended by Nogin [7], Ghorpade and Lachuad [2], Ghorpade, Patil and Pillai [3], Hansen, Jhonsen and Ranestad[4].

Let $G(2,4)$ denote the set of 2 dimensional subspaces of a 4 dimesnional vector space over binary field $F_2=\{0,1\}$.

Let $C(2,4)$ be the linear code associated with $G(2, 4)$ of dimension 4 and of length 16. Let A denote the generator matrix of $C(2,4)$. We give a matrix product construction $[C_1,C_2,,C_l]\ A$ over a binary field.

In this paper, we determine the generator matrix of Grassmann code over binary field. The generator matrix of Grassmann code is a full rank code due to its alge-braic geometric properties. We use this generator matrix and give the Blackmore construction of Matrix product code. We determine the parameters length, dimen-sion and minimum distance of these codes.We also give generator matrix of Grass-mann Matrix product codes.

This paper is organized as follows:

In section 1, we explain the basics of matrix product codes and their known parameters. In section 2, we discuss Grassmnn vari-eties, Grassmann codes. In section 3, we determine the generator matrix of binary Grassmann code G(2,4). Finally, in section 4, we give lower bound for the mini-mum distance of Grassmann codes.

1 Matrix Product Codes

Definition 1: (Matrix Product Codes). Let $C_1, C_2, \cdots, C_l$ be linear codes of length n over F_q. Let $A = (a_{ij})$ be be an $l \times m$ be matrix over F_q. Then the set

$\{[c_1, c_2, \cdots, c_l] \times A : c_i \in C_i$ is $n \times 1$ column vectors, $1 \le i \le l\}$ is called a matrix product code. It is denoted

by $C_A(C_1, C_2, \cdots, C_l)$.

That is, the set of all matrix products $[c_1 c_2 \cdots c_l] \times A$, where $[c_1 c_2 \cdots c_l]$ is of order

$n \times l$ and A is of order $l \times m$. This set is a sub space of $F^{n \times m}$ and q is called matrix product code.

Definition 2: (Code words of Matrix Product Code). A code word of $C_A(C_1, C_2, \ldots, C_l)$ is a matrix of order nm given by:

$$c = \begin{pmatrix} \vdots & \vdots & & \vdots \\ C_1 & C_2 & \cdots & C_l \\ \vdots & \vdots & & \vdots \end{pmatrix} \times \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{l1} & \cdots & a_{lm} \end{pmatrix}$$

$$= \begin{pmatrix} c_{11}a_{11} + c_{12}a_{21} + \cdots + c_{1l}a_{l1} & \cdots & c_{11}a_{1m} + c_{12}a_{21} + \cdots c_{1l}a_{lm} \\ \vdots & \vdots\vdots & \vdots \\ c_{n1}a_{11} + c_{n2}a_{21} + \cdots + c_{nl}a_{l1} & \cdots & c_{n1}a_{1m} + c_{n2}a_{2m} + \cdots + c_{nl}a_{lm} \end{pmatrix}.$$

We can recognize this form of code word as a vector $c = (c_1, c_2, , c_k, , c_{nm})$ of length nm in F_q^{nm}, where the k th entry c_k is the $(r+1, s)$th entry of the above matrix such that $k = rm + s$. That is, divide k by m to get quotient r and remainder s. Then the dot product of $(r+1)$th row of $[C_1 C_2 \cdots C_l]$ and s th column of A gives $c_k \in C$.

1.1 Example of Matrix Product Code

Let $C_1 = \{(0,0,0), (0,1,1)\}$, and $C_2 = \{(0,0,0), (1,1,0)(1,0,1), (0,1,1)\}$ be two codes of length 3 over the binary field and Let $A = \begin{pmatrix} 1\,0\,1\,1 \\ 0\,1\,0\,1 \end{pmatrix}$ be a matrix of order 2×4. Then, the code words of $C_A(C_1, C_2)$ are listed below :

(i). $\begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = (0,0,0,0,0,0,0,0,0,0,0,0) \in F_2^{12}$

(ii). $\begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} = (0,1,0,1,0,1,0,1,0,0,0,0) \in F_2^{12}$

(iii) $$\begin{pmatrix} 0\,1 \\ 0\,0 \\ 0\,1 \end{pmatrix} \times \begin{pmatrix} 1\,0\,1\,1 \\ 0\,1\,0\,1 \end{pmatrix} = \begin{pmatrix} 0\,1\,0\,1 \\ 0\,0\,0\,0 \\ 0\,1\,0\,1 \end{pmatrix} = (0,1,0,1,0,0,0,0,0,1,0,1) \in F_2^{12}$$

(iv) $$\begin{pmatrix} 0\,0 \\ 0\,1 \\ 0\,1 \end{pmatrix} \times \begin{pmatrix} 1\,0\,1\,1 \\ 0\,1\,0\,1 \end{pmatrix} = \begin{pmatrix} 0\,0\,0\,0 \\ 0\,1\,0\,1 \\ 0\,1\,0\,1 \end{pmatrix} = (0,0,0,0,0,1,0,1,0,1,0,1) \in F_2^{12}$$

(v) $$\begin{pmatrix} 0\,0 \\ 1\,0 \\ 1\,0 \end{pmatrix} \times \begin{pmatrix} 1\,0\,1\,1 \\ 0\,1\,0\,1 \end{pmatrix} = \begin{pmatrix} 0\,0\,0\,0 \\ 1\,0\,1\,1 \\ 1\,0\,1\,1 \end{pmatrix} = (0,0,0,0,1,0,1,1,1,0,1,1) \in F_2^{12}$$

(vi) $$\begin{pmatrix} 0\,1 \\ 1\,1 \\ 1\,0 \end{pmatrix} \times \begin{pmatrix} 1\,0\,1\,1 \\ 0\,1\,0\,1 \end{pmatrix} = \begin{pmatrix} 0\,1\,0\,1 \\ 1\,1\,1\,0 \\ 1\,0\,1\,1 \end{pmatrix} = (0,1,0,1,1,1,1,0,1,0,1,1) \in F_2^{12}$$

(vii) $$\begin{pmatrix} 0\,1 \\ 1\,0 \\ 1\,1 \end{pmatrix} \times \begin{pmatrix} 1\,0\,1\,1 \\ 0\,1\,0\,1 \end{pmatrix} = \begin{pmatrix} 0\,1\,0\,1 \\ 1\,0\,1\,1 \\ 1\,1\,1\,0 \end{pmatrix} = (0,1,0,1,1,0,1,1,1,1,1,0) \in F_2^{12}$$

(viii) $$\begin{pmatrix} 0\,0 \\ 1\,1 \\ 1\,1 \end{pmatrix} \times \begin{pmatrix} 1\,0\,1\,1 \\ 0\,1\,0\,1 \end{pmatrix} = \begin{pmatrix} 0\,0\,0\,0 \\ 1\,1\,1\,0 \\ 1\,1\,1\,0 \end{pmatrix} = (0,0,0,0,1,1,1,0,1,1,1,0) \in F_2^{12}$$

1.2 Parameters of Matrix Product Code

From definition 2, we observe that the matrix product code code C is of length nm, and each kth entry c_k in each codeword c is obtained by multiplying $(q+1)$th row of $[C_1,\cdots,C_l]$ and rth column of A, where q and r are such that $k=nq+r$. In [1], it has been proved that if A is non singular matrix then the size of the matrix product code $C_A(C_1,\cdots,C_l)$ is equal to the product $|C_1||C_2|\cdots|C_l|$.

Definition 3. A matrix A is said to be non singular by columns matrix (NSC) if a $t\times t$ minor consisting of any t columns of A is non zero, for $1\le t\le l$.

If we choose A to be NSC, then the minimum distance of matrix product code $C_A(C_1,\cdots,C_l)$ is given by the following theorem due to Blackmore and et al.

Theorem 1: (Minimum Distance of Matrix Product Code). [1] If A is non singular by columns matrix and d(C) denote the minimum distance of C then

$d(C) \geq min\{md_1, (m-1)d_2, \cdots, (m-l+1)d_l\}$,

Where d_i is minimum distance of C_i for $1 \leq i \leq m$.

Moreover, if A is triangular then $d(C) = min\{md_1, (m-1)d_2, \cdots, (m-l+1)d_l\}$.

One can refer to [1] for the detailed proof.

1.3 Grassmannians and Grassmann Codes

Study of Grassmann codes associated with projective Grassmann variety over finite field Fq was initiated by Ryan and Ryan and studied extensively by Nogin, Ghorpade, Lachuad, Patil, Pillai, Hansen, Johnsen, Ranestad [7,2,3, 4]. In this section, we briefly give the introduction about Grassmannians and Grassmann codes.The Grassmannian G(t,s)(V) over a field F is the set of all t dimensional sub spaces of s dimensional vector space V.

We describe Grassmannians as a projective variety as follows: Fix a basis {e1,e2,...es} of V. Let W be a t-dimensional sub space of V . A basis {v1, v2, . . . , vt } of W gives rise to a t×s matrix AW= (aij) of rank t whose rows are coordinates with respect to {e1,e2,...,es} of v1,v2,...,vt.

For any α I(t, s), we let pα(A) be the αth minor of AW by which we mean t× tth minor of AW given by

$$P\alpha(A_W) = \begin{vmatrix} a_1\alpha_1 & a_1\alpha_2 \cdots & a_1\alpha_l \\ a_2\alpha_1 & a_2\alpha_2 \cdots & a_2\alpha_l \\ \vdots & \vdots & \vdots \\ a_1\alpha_1 & at\alpha_2 \cdots & a_t\alpha_l \end{vmatrix}$$

Thereare $\binom{s}{t}$ such $t \times t$ minors. A different choice of a basis of W changes A_W to CA_W where C is some nonsingular $t \times t$ matrix with entries in F. Clearly, $p_\alpha(CA_W) = \det(C) p_\alpha(A_W)$. Therefore, the $\binom{s}{t}$-tuple$(\ldots, p_\alpha(A), \ldots)$ where α varies over $I(t,s)$ is uniquely determined by W up to proportionality.

Thus each $W \in G(t,s)$
is mapped to a unique point in $P^{\binom{s}{t}-1}$. This gives rise to a $G(t,s) \xrightarrow{\pi} P^{\binom{s}{t}-1}$
given by $W \to [\ldots : p_\alpha(A_W) : \ldots]$. This map is called the *Plücker embedding* of
$G(t,s)$ and the coordinates of $\pi(W) = (\ldots, p_\alpha(A_W), \ldots)$ are called the *Plückerco-ordinates* of W. We will The set $\{\pi(W) \in P^{\binom{s}{t}-1} : \pi(W) = (\ldots, p_\alpha(A_W), \ldots)\}$ is a non degenerate projective system in $P^{\binom{s}{t}-1}$ which give a non degenerate linear code under the well known Tsfasman-Vlăduţ correspondence over finite field F_q([9]).This code is called *Grassmann code*.

It is denoted by $C(t, s)$. It has been proved that the length, dimension, and minimum distance of Grassmnn code is:

International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 11 Issue 4, April-2022, Impact Factor: 7.957

$n:=\begin{bmatrix} s \\ t \end{bmatrix}_q$, $k:=\binom{s}{t}$, $d:=q^{\delta}$ respectively,

Where

$$\begin{bmatrix} s \\ t \end{bmatrix}_q = \frac{(q^s-1)(q^s-q)\dots(q^s-q^{t-1})}{(q^t-1)(q^t-q)\dots(q^t-q^{t-1})} \qquad (2)$$

$$\delta := t(s-t) \qquad (3)$$

2 Binary Grassmann Code $C(2,4)$

In this section we work over a binary field F_2 and determine explicitly the generator matrix of Grassmann code $C(2,4)$ over F_2 using Tsfasman-Vlăduţ correspondence.

Consider the Grassmannian $G(2,4)$ of 2 dimensional sub spaces of vector space F^4.
2

Let $\{e_1,e_2,e_3,e_4\}$ *be a fixed basis of* F_2^4. *We know that* $|F_2^4| = 2^4 = 16$.

Since the underlying field is binary field, it is obvious to check that distinct vectors are linearly independent. Hence the span of any two distinct vectors in F_2^4 gives the two dimensional sub space of F_2^4 .Then a two dimensional sub space W of $(2,4)$is of the

$form W = \{\mathbf{u_i}, \mathbf{u_j}, \mathbf{u_i}+\mathbf{u_j} : \mathbf{u_i}, \mathbf{u_j} \in \mathbf{F}_2^4\, u_i \neq u_j\}$ Then by (2), $|G(2,4)| = \begin{bmatrix} 4 \\ 2 \end{bmatrix}_2 = 35$

Hence, we have 35 plucker coordinates in the projective space $P^{\binom{4}{2}-1} = P^5$ listed below:

$P_1=(1,0,0,0,0,0)P_{10}=(1,0,0,1,,0,0)P_{19}=(1,1,0,1,0,0)P_{28}=(1,0,1,1,0,1)$
$P_2=(0,1,0,0,0,0)P_{11}=(1,0,0,0,,1,0)P_{20}=(1,0,1,0,1,0)P_{29}=(1,1,0,0,1,1)$
$P_3=(0,0,1,0,0,0)P_{12}=(0,0,0,1,,1,0)P_{21}=(0,0,0,1,1,1)P_{30}=(0,1,1,1,1,1)$
$P_4=(0,0,0,1,0,0)P_{13}=(0,1,0,1,,0,0)P_{22}=(0,1,1,0,0,1)P_{31}=(1,1,1,0,1,1)$
$P_5=(0,0,0,0,1,0)P_{14}=(0,1,0,0,,0,1)P_{23}=(1,1,1,0,0,0)P_{32}=(1,0,1,1,1,1)$
$P_6=(0,0,0,0,0,1)P_{15}=(0,0,0,1,,0,1)P_{24}=(1,0,0,1,1,0)P_{33}=(1,1,1,1,0,1)$
$P_7=(1,1,0,0,0,0)P_{16}=(0,0,1,0,,1,0)P_{25}=(0,1,0,1,0,1)P_{34}=(1,1,0,1,1,1)$
$P_8=(1,0,1,0,0,0)P_{17}=(0,0,1,0,,0,1)P_{26}=(0,0,1,0,1,1)P_{35}=(1,1,1,1,1,0)$
$P_9=(0,1,1,0,0,0)$ $P_{18}=(0,0,0,0,,1,1)P_{27}=(0,1,1,1,1,0)$

This proves the following theorem.

Theorem 2. *[Generator Matrix of Binary* $C(2,4)$*] The generator matrix of* $C(2,4)$
Of order 6×35 *isgiven by*

$$\left[I_6 \mathrm{M} P_7^t\, p_8^t \mathrm{L}\ \ p_{35}^t \right] \qquad (4)$$

3 Minimum Distance of Binary Grassmann Matrix Product Codes

In this section we use the Blackmore construction of matrix product code for a generator matrix matrix G of binary Grassmann code $C(2, 4)$ and give formula for minimum distance of corresponding matrix product codes. Following theorem gives the minimum distance of binary Grassmann Matrix product code.

Theorem 3. Let C1,C2,,C6be binary linear codes of lenth 6 and let G be the generator matrix of the binary Grassmann C(2, 4) given by theorem (2). Then minimum distance

Proof. The Grassmannian $G(2, 4)$ over F_2 as a projective variety is a subset of pro-jectivespaceP^5. The Plucker coordinates under the Plucker embedding form a $[35, 6]_2$- projective system. Therefore, by the Ts afasmann-Vladut correspondence, there exists a $[35, 6]_2$ linear code $C(2, 4)$. Since the Plucker embedding is indeed an embedding, therefore, there does not exists any i such that the ith entry is zero forall code words. This shows that the code $C(2, 4)$ is non degenerate. That is, it is not contained in any coordinate hyper plane.

Hence, the generator matrix of this code is full rank matrix. Also, the minimum distance of $C(2, 4)$ over F_2 is $d = 2^{\delta}$. Here $\delta=2$ (4 2)≤≤4.Therefore,$d=2^4=16$.

Let d_i, 1 i6 be the minimum distance of linear codes C_i, 1 i 6. Then, by theorem 1, the minimum distance of $C(2, 4)$is $d\geq\min\{35d_1,34d_2,33d_3,32d_4,31d_5,30d_6\}$ (5)

REFERENCES

[1]. Blackmore,T.,Norton,G.H.:Matrix-ProductcodesoverF_q.AAECC**12**,477–500(2001)

[2]. Ghorpade,S.R. ,LachaudG.: Higher weights of Grassmann Codes.Coding Theory, Cryptog-raphy and Related Areas (J. Buchmann, T. Hoeholdt, H. Stictenoth, and H. Tapia - Resillas,Eds.)Springer-Verlag,Heidelberg,Germany,120–131(1995)

[3]. Ghorpade, S.R., Patil, A.R., Pillai, H.P.: Decomposable subspaces, linear sections of Grass-mannvarieties ,and higher weights of Grassmanncodes. FiniteFieldsandTheirApplications**15**,54–68(2009)

[4]. Hansen,J.P., Johnsen, T., Ranestad, T.K.: Grassmann codes and Schubertunions. Arithmetic, Geometry and Coding Theory, AGCT-2005, Luminy(2005)

[5]. Hernando,F., Lally,K., Ruano,D.: Construction and decoding of matrix-product codes from nested codes. Appl. Algebra Engrg. Comm. Comput. **20**,497–507(2009)

[6]. Mac Williams, F.J., Sloane,N.J.A.:The theory of error-correcting codes. Elsevier, Amster-dam(1977)

[7]. Nogin, D. Yu.: Codes associated to Grassmannians. Arithmetic, Geometry and Coding The-ory,145–154(1996)

[8]. Ozbudak,F., Stichtenoth, H.,:NoteonNeiderreiter-X inf's propagation rule for linear codes.Appl.Algebra Engrg.Comm. Comput. **13**,53–56(2002)

[9]. Patil, A.R.: Note on Neiderreiter - Xinf's propagation rule for linear codes. Appl. AlgebraEngrg.Comm.Comput.**13**,53–56(2002)

[10]. Ryan,C.T.:ProjectivecodesbasedonGrassmannvarieties.Congr.Numer.**57**,273–279(1987)

[11]. Tsfasman, M.A., Vlăduţ, S.G.: Geometric approach to higher weights. IEEE Trans .Inform. Theory **40**,1564–1588(1995).