International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 11 Issue 5, May-2022, Impact Factor: 7.957

Squares of codes associated to Grassmannians over F2

Dattatraya Sadashivrao Mangnale

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

ABSTRACT

In this paper we develop the formalism of product of linear codes under component wise multiplication. The square C^{*2} of a linear error correcting code C is the linear code spanned by the coordinate-wise products of every pair of (non necessarily distinct) word sin Grassmann binary code C is studied.

Product of linear codes

Schur Product: Let F be any field and an integer n1. Let de note componen-twise multiplication in F^n,i.e.

$$(x_1,x_2,\cdots,x_n)*(y_1,y_2,\cdots,y_n)=(x_1y_1,\cdots,x_ny_n). \quad \geq \quad *$$

This is also called Schur Product. Let C, D be linear codes over F_q, then we define their product $C*D$ as the set

$$\{c*d:c\in C,d\in D\}$$

Example Consider the codes $C=\{(0,0,0,0),(1,0,1,1),(0,1,1,0),(1,1,0,1)\}$and

$D=\{(0,0,0,0),(1,0,0,0),(0,1,1,1),(1,1,1,1)\}\subseteq \mathrm{F}^4$then the product is given by

$C*D=\{(0,0,0,0),(1,0,0,0),(0,0,1,1),(1,0,1,1),(0,1,1,0),(0,1,0,1),$
$(1,1,0,1)\}$.

Proposition 0.1(Bounds on dimension and min. distance)*(i)*$dimC\leq dimC^{*2}\leq$

$$\frac{(dimC).(dimC+1)}{2}$$

(ii)$d(C^{*2})\leq d(C)$

Proof Let dim $C=k$,fix the basis $g_1,g_2,\ldots,g_k$ for C. The corresponding F_q system of generators for $C^{*2}$is $g_i\{ * \{g_j:1\leq i \leq j \leq k\}\}$,therefore, –

$\dim(C^{*2})\leq|\{g_i*g_j:1\leq i\leq j\leq k\}|$.

Corresponding to g_1, we obtain k generators of the formg_1*g_j, for$g_2$we get $k-1$ generators g_2*g_j, and soon. Thus, the total number of generators

$g_i*g_j;(1\leq i\leq j \leq k)$isequalto$k+(k-1)+\ldots+3+2+1=\frac{k(k+1)}{2}$hence

$$dimC^{*2}\leq\frac{k(k+1)}{2}=\frac{(dimC).(dimC+1)}{2}$$

Now, themap$c\mapsto c*c$isinjective,anditisclearthat$C\subseteq C^{*2}$,thereforedim$C\leq$

$dimC^{*2}\ldots$(2).Ther fore from(1)and(2)weget$dimC\leq dimC^{*2}\leq\frac{(dimC).(dimC+1)}{2}$

Proposition 0.2(Singleton-like Bound) *It hold sthatd* $(C^{*2})\leq max\{1,n-2dimC+2\}$
Note: For very small dimension of$C$or$C^{*2}$the boundi sachieved.

Proposition 0.3*Suppose that* $d(C^{*2})>1$. *If* $d(C^{*2})=n \quad 2dimC+2$ *, then C is either a Reed-Solomon code or a direct sum of self-dual codes, where self duality is relative to a non– degenerate bilinear form which is not necessarily the standard inner product. Furthermore, if in addition* $dimC2$ *and* $d(C^{*2}) \quad 3$ *, then C is a Reed-Solomon code.*

Squares of Reed-Solomon codes are infact ag a in Reed-Solomon codes. Given integers$0\leq m<n$, a finite field F of cardinality$|\mathrm{F}|\geq n$ and avector$b=(b_1,b_2,\ldots,b_n)\in \mathrm{F}^n$

Of evaluation points under the condition that $b_i \neq b_j$ if $i \neq j$, the Reed-Solomon code $RS_{F,b}(m, n)$ is defined as $RS_{F,b}(m, n) = \{(f(b_1), f(b_2), \ldots, f(b_n)) : f \in F[X], \deg f \leq m\}$ and it is a code of dimension $m + 1$ and minimum distance $n - m$. We have that $(RS_{F,b}(m, n))^{*2} = RS_{F,b}(2m, n)$, as long as $2m < n$. Otherwise $(RS_{F,b}(m, n))^{*2} = RS_{F,b}(n-1, n) = F^n$.

Lemma 0.4 *Let $v_0 \in (F_q^*)^m, v_1, v_2, \ldots, v_h \in F_q^m$. If $v_1, \ldots, v_h$ are linearly independent over F_q then $v_0 * v_1, \cdots v_0 * v_h$ are linearly independent over F_q*

Proof Let $v_{i,j}$ denote the j^{th} co-ordinate of the vector v_i. Let $\alpha_1, \alpha_2, \ldots, \alpha_h \in F_q$ be such that

$$\sum^{h} \alpha_i v_0 * v_i = 0 \qquad (1)$$

then for all $j = 1, \ldots, m$

$$\sum_{i=1}^{h} \alpha_i v_{0,j} v_{i,j} = 0 \Longrightarrow \sum_{i=0}^{h} \alpha_i v_{i,j} = 0, \qquad (2)$$

as $v_{0,j} \neq 0$; therefore $\sum_{i=1}^{h} \alpha_i v_i = 0$ and since the v_i's are linearly independent this yields $\alpha_i = 0$ for all $i = 1, \cdots, h$.

Corollary 0.5 *Let C be an MDS $[n,k]_q$ code. If $2k-1 \leq n$ then the dimension of product $k^* \geq 2k - 1$.*

Proof Let G be a generator matrix for C, written as

$$\begin{pmatrix} 1 & & & \\ & \ddots & & |G' \\ & & 1 & \end{pmatrix}$$

Where $G' \in M_{k,n-k}(F_q^*)$ (by MDS hypothesis). The MDS hypothesis and $2k-1 \leq n$ imply that $k \leq d$, which implies that any $k - 1$ rows of G' are linearly independent. Hence we can apply the previous lemma choosing as $v_0, \ldots, v_{k-1}$ any set of rows and conclude.

Example Let $k \leq n \leq q$, fix n distinct elements $x_1, \ldots, x_n \in F_q$ and let C be the Reed-Solomon $[n,k]_q$ code generated by the matrix

$$G = \begin{pmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_n \\ \vdots & & \vdots \\ x_1^{k-1} & \cdots & x_n^{k-1} \end{pmatrix}$$

Then C * is generated by

$$G^* = \begin{pmatrix} 1 & \cdots & 1 \\ x_n & \cdots & x_n \\ \vdots & & \vdots \\ x_1^{2k-2} & \cdots & x_n^{2k-2} \end{pmatrix}$$

in perticular , $rkG* = \min\{2k - 1, n\}$. Hence , if $2k - 1 \leq n$, $C*$ is a Reed-Solomon $[n, 2k - 1]_q$ code.

Grassmanians and Grassman codes

The Grassmanian G`,m(F) is the set of `− dimensional linear subspace of a m− dimensional vector space over a field F.

If F = Fq then we can find its cardinality $|G_{l,m}(Fq)|$ which is given by $|G_{l,m}(Fq)|$ =

$$\begin{bmatrix} m \\ l \end{bmatrix}_q = \frac{(q^m-1)\,(q^m-q)\ \cdots(q^m-q^{l-1})}{(q^l-1)\,(q^l-q)\cdots(q^l-q^{l-1})}$$

Grassmannians as a projective variety can be viewed as follows:

Fix a basis {e1, e2, . . . ,em} of V . Let W ∈ Gl,m and let {v1, v2, . . . , v`} be a basis of W . This basis gives rise a $l$×m matrix Aw = (aij ) of rank$l$. Now, fix the indexing set I($l$, m) = {α = (α1, α2, . . .$\alpha_l$) ∈$Z^l$: 1 ≤ α1 ≤ . . . ≤ α` ≤ m} be an indexing set [ordered , say lexicographically] for the points of p_k^q .Given any α ∈ I(l, m) and any$l$ × m matrix A = (aij) , let pα(a) = α − th minor of A :=det(aiαj)1 ≤ i; j ≤ l.then p(W) = (pα(AW))α∈I(l,m) ∈$p_{\mathrm{Fq}}^{k-1}$is called Plücker co-ordinate of W . The map W → p(W) of Gl,m(Fq) →p_{Fq}^{k-1} is an injective map and its image equals the zero of locus of certain quadratic polynomials ,this map is then called as Plücker embedding.

Grassman Code:

The non degenerate [n, k]q -code corresponding to the projective system defined by $G_{l,m}$(Fq) (with its Plücker embedding) is denoted by C(l, m) and is Grassman Code.

Computing C(2, 4)∗2

C(2, 4)(F2) is the Grassmann code obtained from Grassmannian G(2,4)(F2), The Plucker coordinates of G(2, 4) in P_{F2}^5have been computed here:

p1 = (1, 0, 0, 0, 0, 0), p2 = (0, 1, 0, 0, 0, 0), p3 = (0, 0, 1, 0, 0, 0), · · · p35 = (1, 1, 1, 1, 1, 0)

These Plucker coordinates gives us a generator matrix of order 6×35 given below:

$$\begin{pmatrix} \vdots & \vdots & \vdots & \cdots & \vdots \\ p_1 & p_2 & p_3 & \cdots & p_{35} \\ \vdots & \vdots & \vdots & \cdots & \vdots \end{pmatrix}$$

The dimension k of this code is 6 and the length n is 35. Here, we have calculated the dimension of C ∗2 as 21 and computed the generator matrix of order 6 × 35.

REFERENCES

[1]. C.T. Ryan, An application of Grassmann varieties to Coding Theory, Congr. Numer.57(1987),257-271
[2]. C.T. Ryan, Projective codes based on Grassmann varieties , Congr. Numer.57(1987),237-279.
[3]. I. Cascudo, On Squares of cyclic codes, IEEE Trans. Inform. Theory, 65(2) (2019), 1034-1047.