IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 19, Issue 3 Ser. I (May. – June. 2023), PP 39-43
www.iosrjournals.org

On The 2-Traceability Property Of Hadamard Matrices

Anu Kathuria
Assistant Professor, The Technological Institute of Textile and Sciences,Bhiwani.

Abstract:*The concept of tracing the pirated copy of Digital content was introduced by Chor, Fiat and Naor [5]in 1994.Then the Strong form of Codes*
i.e. traceable codes was defined by Staddon and Wei[9]in 2001. Several authors defined different combinatorial structures like Hadamard Codes, t-Designs, and Balanced Incomplete Block Designs in form of frameproof and traceable (TA) codes. Here in this present study we show that Hadamard Codes with parameters $(n-1, n, \frac{n}{2})$ *obtained from HadamardMatrices are not in general 2-TA. We also show that the rows of Hadamard matrices of the type* $(n, n, \frac{n}{2})$ *do not form 2-TA.*

Keywords *: Balanced Incomplete Block Design,Hadamard Code and Hadamard Matrix, Traceable (TA) Code*

Date of Submission: 14-05-2023 Date of Acceptance: 24-05-2023

I. Introduction:

Before being sold any copy in the market a merchant embeds some codeword into the copy to prevent illegal data redistribution and digital data piracy. This marking allows the distributor to trace down and return any unauthorised copy to the intended receiver. With this in mind, a user may be wary to reproduce something without permission. However, if a group of dishonest users set out to identify some of the signs and devise a new codeword, they could be able to create a new copy that stands out from the rest. In 1994, Boneh and Shaw [3] suggested the concept of frameproof codes to prevent them from doing so because they have the ability to make markings at will.A c- frameproof code has the characteristic that no coalition of at most c users may frame a non-participant in the piracy.

II. Preliminaries

Through out the paper ,the following definitions and terminology will be used and F_q denotes a finite field with q elements.

Here we recall some basic definitions related to error correcting codes.

(i) Let Q be a finite set of alphabets. Then a subset C C Q^n is called a code of length n over Q. The elements of Q^n are called words and the elements of C are called codewords of length n.

(ii) Let a and b be two codewords ,then the hamming distance between a and b d(a,b) is the number of coordinates in which they differ and the number of non zero coordinates of a word c is called the weight of c.The minimum distance d of C is d=min.{d(a,b)| a,bϵC}.

(iii) I(x,y)={i: $x_i = y_i$} for x={ $x_1, x_2 \ldots\ldots x_n$} , y={$y_1, y_2 \ldots\ldots y_n$}$\epsilon Q^n$. Similarly we can define I(x,y,z…..)for any number of words x,y,z…..

Now let us define some terms related to fingerprinting codes

(i) Detectable and Undetectable Positions: Let X is a subset of Q^n. Then we say that the position iϵQ^n is undetectable for X if ith position of each word x ϵ X is occupied with the same alphabet, otherwise the position is detectable.

(ii)Coalition: it means two or more users meet for the purpose of creating an illegal copy of a digital object (see Marking Assumption (iv) also)by comparing their copies. A member of the coalition is called a pirate.

(iii) Descendant Set: For any two words a = {a_1 ,a_2,……..a_n} and

b={b_1,b_2……b_n} in Q^n,the set of descendants is defined

D(a,b) = {x ϵQ^n | $x_i \epsilon$ { a_i,b_i},i=1,2,3…n.The above definition of descendant set can be naturally extended to any finite number of words a, b, c……

(iv) Marking Assumption: In the static form of fingerprinting scheme each digital content is divided into multiple segments, among which n segments are chosen for marking them with symbols which correspond to alphabets in Q. Each user receives a copy of the content with differently marked symbols .if a code C over Q of

length n is used to assign the symbols for each segment to each user. Then each copy can be denoted as Codeword of C and each coordinate x_i of a codeword $\{x_1,x_2,\ldots.x_n\}$can be termed as symbol. Further assume that any coalition of c users is capable of creating a pirated copy whose marked symbols correspond to a word of Q^n that lie in the Descendant set of c users.

(v) Traceable Code: For x,y ϵ Q^n;define I(x,y)={i : $x_i = y_i$ }. C is c-TA code provided that for all I and for all x ϵ $desc_c(C_{i)}$) there is atleast one codeword
yϵ$C_i(C_i$ C) ; $|(x,y)|>|(x,z)|\ for\ any\ z\epsilon\ C/C_{i..}$ The condition in terms of
distance is equivalent to d(x,y) < d(x,z).

(vi)Frameproof Code: A (v,b)-code T is called a c-frameproof code if ,for every W ⊂ T such that $|W| \leq c$, we have F(W) ∩ T=W. We will say that T is a c-FPC (v,b) for short. Thus, in a c-frameproof code the only codewords in the feasible set a coalition of at most c users are the codewords of the members of the coalition. Hence, no coalition of atmost c users can frame a user who is not in coalition.
Example 2.3.1: Let S be a code given by
S= {(4,2,3),(0,7,0),(0,4,9)} and
W={(4,2,3),(0,7,0)} is the set of colluders. Suppose these colluders collude and generate a new codeword (4, 7, 0), By the definition of TA-code in (v),
d {(4,7,0) and (0,7,0)} = 1.So it can be easily concluded that the colluder with the codeword (0,7,0) is the actual culprit. He can easily be traced.
Example 2.3.2: Let S be a code given by
S={(7,0,0),(7,6,0),(0,0,8),(7,6,8)} and
W={(7,6,0),(0,0,8)} by the definition of feasible set given above
F(W)={(7,6,0),(0,0,8),(7,6,8),(7,0,0) }
Here F(W) ∩S≠W. So the above code is not a 2-frameproof code.

Theorem [3]: Let C be a c-frameproof code and D be an $(n,M,d)_q$- Error Correcting Code. If T be the composition of C and D ,Then T is a c-frameproof code ,provided $d > \left(1-\frac{1}{c}\right)n, c = 2,3,4 \ldots \ldots \ldots$

Hadamard Code as 2-FP Code: In this Section we show that "Hadamard Codes with parameters $(n-1,n,\frac{n}{2})$ are 2-FP Codes in general".Before discussing it in detail ,we recall a few definitions.
Definition 3.1[10.]: A Hadamard Matrix Mis a square matrix of order n with every entry equal to 1 or -1 such thatMM^T= nI,where M^T denotes the transpose of matrix M.
Definition 3.2[10.]: A Hadmard Matrix A of order n in which every entry in the first row and in the first column is +1 is called N**ormalized Hadamard Matrix** of order n.
Example 3.2.1: The normalized Hadamard Matrix of order 2 is

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Proposition[10]: if M is a Hadamard matrix of order n then

$$\begin{bmatrix} M & M \\ M & -M \end{bmatrix}$$

is a Hadamard matrix of order 2n.

Theorem 3.2.2[10]: if a Hadamard matrix of order n exists ,then n = 1,2 or a multiple of 4.

Definition 3.3 [10.]: A matrix obtained from Hadamard matrix M_n of order 'n' by changing 1's into 0's and -1's into 1's is called Binary Hadamard matrix of order n,let us denote it with A_n.
Definition 3.4[10.]: Equidistant Constant Weight Code: A code S is called Constant Weight Code if all the codewords have the same weight. A code is called equidistant if the distance between any two codewords is same. Acode S having both properties is called Equidistant Constant Weight Code. In [7] Gerard Cohen,claims that Hadamard Codes with parameters $(n-1,n,\frac{n)}{2})$ are 3-FPC.Here in this section we show that Hadamard prove to be a 2-frameproof code ? In this context here we represent a Theorem.
Theorem 1: Hadamard Codes with parameters $(n-1,n,\frac{n)}{2})$ is always a 2-FP Code. Here length of the code is (n-1). The size of the code is n and distance d of the code is $n/2$.
Proof : let A_n be a normalized Hadamard Matrix of order n and B_n be the Binary

Hadamard Matrix of order n obtained from $A_{n.}$. Since any two rows of A_n are orthogonal, therefore any two rows of $A_{n.}$agree in $\frac{n}{2}$ places and differ in the remaining $\frac{n}{2}$places . So it follows that

(i) the distance between any two rows ofB_n is $\frac{n}{2}$.

(ii) the weight of every non-zero row of B_n is $\frac{n}{2}$.

So by the definition 1.4[10] of Equidistant Constant Weight Code,

Binary Hadamard Matrix B_n given by $(n, n, , \frac{n}{2})$ is Equidistant Constant Weight Code. Also we can observe that every row of B_n has first entry zero. Let C_n be the matrix obtained from B_n ,with first entry of every row deleted.Then the matrix C_n has n elements of length (n-1),and distance between any two rows of B_n is n/2. The matrix C_n so obtained is called Hadamard Code of type $(n-1, n, \frac{n}{2})$.Now we show that it is2-frameproof code .Since for this code d= $\frac{n}{2}$and$l = n-1$. Therefore by the definition of frameproof [3] of frameproof code $d > (\frac{l}{2})$ i.e. d > (1- $\frac{1}{2}$)l $(should\ be)$. So here the above definition holds and so, Hadamard Codes with parameters$(n-1, n, \frac{n}{2})$ is 2-FP Code.

Example 1.1: Let us consider a normalized Hadamard Matrix of order 4 given as ;

$$A_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

Then as discussed above,the matrix C_4 will be

$$= \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

So it is a Hadamard Code of length 3 with n=4 and distance d is 2.

Therefore by the definition[3] of frameproof code ,$d > \left(1 - \frac{1}{2}\right) n$ i.e. $d > \frac{3}{2}$. So it is 2-FP code.

Now here we discuss necessary and sufficient conditions for an equidistant code to be 2-TA code.

Lemma [1]: An equidistant code of length n with $n - 3s + 2l > 0$ for all a,b ,c $\in C$ is always a 2-TA code.

Lemma [1]:Let C be an equidistant code of length n such that $n - 3s + 2l = 0$ for some a,b,x $\in C$, then C is not a 2-TA code .(s is equal to that number where any two codewords match i.e. distance and l defines that number where any three codewords match.

Proposition[11]:Let C be a binary ,linear and equidistant code with parameters [n,k,d]. Let u,v,w $\in C - \{0\}$, then $|S(u) \cap S(w) - S(u) \cap S(v)| = |S(w) \cap S(v)) - (S(u) \cap S(v))| \leq \frac{d}{2}$

In view of the above results available in literature and the results proved by us in [1] now we are in the state of proving a theorem.

Theorem 2: We propose that for a Hadamard Matrix of O(n);any three codewords match at $\frac{n}{4}$ positions and for such code $n - 3s + 2l = 0$.

Proof : As we have just shown above that distance d between any two codewords of Hadamard Code is $\frac{n}{2}$ and it can be easily verified using the result of above proposition that any three codewords of Hadamard Code match at $\frac{n}{4}$ positions.

As it is equidistant code also so if we use the above condition of 2-TA.then we note that the equation $n - 3s + 2l = 0$(i.e. $n - 3\ (\frac{n}{2}) + 2(\frac{n}{4}) = 0$)

By the definition for a code C to be 2-TA, $n - 3s + 2l > 0$(should be).it verifies that Hadamard Code with parameters $(n-1, n, \frac{n}{2})$cannot be 2-TA.Here we represent anexample also

Example: Let H be a Hadamard matrix of order 8 given by,

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}$$

Now on replacing each 1 with 0 and -1 with 1,as discussed above we get

that $C_8' = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$

So it is a Hadamard Code H with parameters (7,8,4)as discussed above. Now we show that it is not 2 – TA .Let each codeword of this matrix H is

assigned as codewords a,b,c,d,e,f, g and h.if any three users with codewordsb,c collude, i.e.

W= {b, c} with

b =1 0 1 0 1 0 1

c =0 1 1 0 0 1 1

Then by the definition of feasible set [3] defined above ,

F(b,c) = {(0 1 1 01 0 1),(1 0 1 0 0 0 1),

(0 0 1 0 0 0 1)……..}

for our results let the set of colluded words is denoted with i , j and k .

d (a , i) = 4 ,d (b , i) = 2 ,d (c ,i) = 2 ,d (d ,i) = 4 , d (e, i) = 4 ,d (f , i) = 6 ,

d(g , i) = 2, d (h , i) = 4. So it is easy to verify that here innocent user g can also be traced. Although he did not participate in any scheme. This verifies our result.

Even by the sufficient definition [3] of frameproof code ,it is not 2-TA.For such codewords $n - 3s + 2l = 7 - 3(3) + 2(1) = 0$.

3.3.2. Plotkin Bound [10]**:** Let M be a Code of length n, size F and minimum distance d over Q with c elements then d $\leq \frac{nF(c-1)}{(F-1)c}$. If

$d = \frac{nF(c-1)}{(F-1)c}$,then the above code M is Optimal also.

Theorem 3: We claim that Hadamard Codes with parameters $(n-1, n, n/2)$ is Optimal Equdistant Constant Weight Code.

Proof : As we have just shown above that Hadamard Codes with parameters $(n-1, n, n/2)\ is$ Equidistant Constant Weight Code .Here we show that it satisfies Plotkin Bound also.Since here length of the code is $(n-1)$, no. of codewords are n and distance d of the code is $\frac{n}{2}$.Size m of the code is 2 i.e.

(q=0,1).On combining above results we can say that Hadamard codes with parameters $(n-1, n, n/2)$ is Optimal Equidistant Constant Weight Code.

Here in this section we show that rows of a Hadamard Matrix cannot be 2-TA .

Lemma.4.1[1]: Let C be an equidistant code of length n such that $n - 3s + 2l = 0$ for some $a, b, x \in C$,then C is not 2- TA Code.

The above result can be used in proving any code not to be 2-TA.Here we also notice that result is true for a Hadamard Matrix $n - 3s + 2l = 0$;in above examples.Here n is the length of the codeword,s defines those number of places where any two codewords match and l defines those number of places where any three codewords match.

Theorem 4: We propose that any three codewords of a Hadamard Matrix of order n, match at $\frac{n}{4}$ positions.(i.e. $l = \frac{n}{4}$)

Proof : As we know that in a Hadamard matrix of order n, 1's and -1's appear equal number of times(o(H)=2n) and satisfy the property that sum of elements of each row and each column is zero. So in case of any three rows the possibilities at different places of codewords will be (1,-1,1) and (-1,-1,1).So at remaining

positions except at the first place of first column of H the elements will match. Moreover the distance between any two rows of a Hadamard matrix of order n is always $\frac{n}{2}$ .So to retain this property distance d among any three codewords of a Hadamard matrix is $\frac{n}{4}$.

Theorem 5: For the rows of Hadamard Matrix of order $n, n-3s+2l=0$,
For some a,b,x $\in C$,then $C$is not 2-TAcode.
Proof: For a given Hadamard matrix of o(n);distance d between any two codewords is always $\frac{n}{2}$;(so $s=\frac{n}{2}$ here)and distance d among three rows of a Hadamard Matrix is always $\frac{n}{4.}$. So the sufficient condition for an equidistant code to be not 2-TA(3-FP)code is also satisfied.

III. Conclusion:

(i) In this paper we show that Hadamard Code with parameters
$(n-1\ , n, \frac{n}{2}\ )$ in not a 2-TA Code.
(ii) Hadamard Codes with parameters $(n-1, n, \frac{n}{2}\ )$ is always an Optimal Equidistant Constant Weight Code.
(iii)The rows of a Binary Hadamard Matrix does not constitute 2-TA Code

IV. Acknowledgements:

Iam thankful toTIT&S;BHIWANI for regular support and encouragement.

References:

[1]. Anu Kathuria, Sudhir Batra and S.K. Arora "On traceabilty property of Equidistant codes" Discrete Mathematics,Elsevier,vol.340,issue 4,April 2017,pg.713-721
[2]. D. Boneh and J. Shaw,"Collusion –Secure fingerprinting for DigitalData",IEEE Transactions on Information Theory,vol.44,pp.1897-1905,1998.
[3]. D. Boneh and J. Shaw,"Collusion –Secure fingerprinting for Digital Data",in Advances in Cryptology-CRYPTO'95, (Lecture Notes in Computer Science)",vol. 963,pp.453-465, New York, 1995.
[4]. Hongxia Jin,Mario Blaum," Combinatorial Properties of Traceability Codes using Error Correcting Codes" IEEE Transformations on Information Theory,vol.53,no.2, February 07.
[5]. B. Chor, A. Fiat and M. Naor,"Tracing Traitors", in Advances in Cryptology – CRYPTO 94 (Lecture Notes in Computer Science)Berlin, Germany, Springer Verlag, vol. 839, pp. 257-270,1994.
[6]. Gerard Cohen, Encheva Sylvia "Frameproof Codes against coalition of pirates" Theoretical Computer Science,vol.273(2002),pp.295-304.
[7]. Gerard Cohen,S. Encheva," Some new p-array Two Secure frameproof Codes"Applied Mathematical Letters 14(2001);pp.177-282
[8]. H.D.L.Hollman ,Jack H. Van Lint ,Jean-Paul Linnartz"On codes with the identifiable Parent Property " Journal of Combinatorial Theory,Series A-82,pp. 121-133,1998.
[9]. J.N. Staddon ,D.R. Stinson,R. Wei," Combinatorial Properties of frameproof and Traceable Codes" IEEE Transactions on Information Theory, vol.47, pp. 1042-1049,2001.
[10]. L.R.Virmani," The Theory of Error Correcting Codes",Chapman and Hall/CRC
[11]. Marcel Fernandez ,Miguel Soriano"Equidistant Binary Fingerprinting Codes: Existence and Identification Algorithm