International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

# A Note about the Property of Frameproof Codes

**Anu Kathuria**

Assistant Professor, The Technological Institute of Textile and Sciences, Bhiwani, India
*anu_sept24[at]rediffmail.com*

**Abstract:** ***Chor, Fiat, and Naor[5 ] established traitor tracing codes in 1994 to secure Digital Content. Boneh and Shaw[3 ] proposed frameproof codes to prohibit privacy in 1994, and they also proposed c-secure codes with $\epsilon$-error, which means that a traitor may be traced from an unlawful copy with a high likelihood. Hadmard Codes, t-Designs, and Balanced Incomplete Block Designs are all examples of frameproof and traceable code structures covered in this work (BIBD).Here in this work i show that Hadmard Code obtained from Hadmard matrix is not a 3-FPC.***

**Keywords:** Balanced Incomplete Block Design, Hadmard Code and Hadmard Matrix

## 1. Introduction

Before being sold, each copy is stamped with a codeword to prevent illegal data redistribution and digital data copying. This marking allows the distributor to trace down and return any unauthorised copies 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. Let v and b be positive integers (b denotes the number of users in the scheme). A Set T=$\{w^{(1)}, w^{(2)}, \ldots \ldots w^{(b)}\}$ C $\{0,1\}^v$ is called a (v,b)-code, and each $w^{(i)}$ is called a codeword. So a codeword is a binary v-tuple. We can use a (b x v) matrix S to depict a (v,b)-code ,in which each row of S is a codeword in T.

Let T be a (v,b)-code. Suppose
C =$\{w^{(u_1)}, w^{(u_2)}, \ldots\ldots, w^{(u_d)}\}$ . Then

For i ∈ {1,2,3……v}, we say that bit position i is detectable for C if

$$\{w_i^{(u_1)} = w_i^{(u_2)} = \ldots\ldots\ldots\ldots w_i^{(u_d)}\}.$$

Let $u(C)$be the set of undetectable positions for C. Then
F(C)= { w ∈ $\{0,1\}^v$ : $\{w | u(C) = w^{(u_i)} | u(C) \; for\ all\ w^{(u_i)} \in C\}$
is called feasible set of C. if $u(C)$=∅ , then we define F(C)= $\{0,1\}^v$ .The feasible set C also represents the set of all possible v-tuples that could be produced by the coalition C by comparing the d codewords they jointly hold. if there is a codeword $w^{(j)} \in F(C) \setminus C$, then user j could be framed in this case.

Definition 1.1 [3]: A (v,b)-code T is called a c-frame proof code if ,for every W ⊂ T such that $|W| \le c$, we have F(W) ∩ T=W. We will say that T is a c-FPC (v,b) for short. Thus, in a c-frame proof code the only code words in the feasible set a coalition of at most c users are the code words of the members of the coalition. Hence , no coalition of atmost c users can frame a user who is not in coalition.

Example 1.1.1: Let C be a code given by
C= {(1,0,0),(0,2,0),(0,0,3)} and
W={(1,0,0),(0,2,0)} , By the definition,
F(W)={(1,2,0),(0,0,0),(1,0,0),(0,2,0)},
i.e. F(W) ∩ C=W.

Example 1.1.2: Let C be a code given by
C={(1,0,0),(1,2,0),(0,0,3),(1,2,3)} and
W={(1,2,0),(0,0,3)} by the definition of feasible set given above
F(W)={(1,2,3),(0,2,3),(1,0,3),(0,0,3),(0,2,0),(1,2,0),(1,0,0),(0,0,0) }
Here F(W) ∩ C ≠ W. So the above code is not a 2-frameproof code.

**Section 1**

**Hadmard Code as 2-FP Code**: in this section we show that "Hadmard Codes in general are also 2-FP Codes". Before discussing it in Detail, we recall its Definition.

Definition 1.1 [10.]: A Hadmard matrix M is a square matrix of order n with every entry equal to 1 or -1 such that $MM^T$= I, where $M^T$ denotes the transpose of matrix M.

Definition 1.2 [10.]: A Hadmard matrix of order n in which every entry in the first row and in the first column is +1 is called Hadmard matrix of order n.

Example 1.2.1: The normalized Hadmard matrix of order 2 is

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

Definition 1.3 [10.]: A matrix obtained from Hadmard matrix $M_n$ of order 'n' by changing 1's into 0's and -1's into 1's is called Binary Hadmard matrix of order n,let us denote it with $A_n$.

Definition 1.4[10.]: Equidistant Constant Weight Code: A code C 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. A code C having both properties is called Equidistant Constant Weight Code.

In this paper we are discussing that How Hadmard Codes prove to be a 2-frameproof code? In this context here we represent a Theorem.

Theorem 1.3.1: Hadmard Code 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 $M_n$ be a normalized Hadmard Matrix of order n and $A_n$ be the Binary

Hadmard Matrix of order n obtained from $M_n$.. Since any two rows of $M_n$ agree in $\frac{n}{2}$ places. So it follows that

(i) Distance between any two rows on $A_n$ is $\frac{n}{2}$.
(ii) Weight of every non-zero row of $A_n$ is $\frac{n}{2}$.

So by the definition 1.4 [10 ] of Equidistant Constant Weight Code, Binary Hadmard Matrix $A_n$ given by (n, n, $\frac{n}{2}$) is Equidistant Constant Weight Code. Also we can observe that every row of $A_n$ has first entry zero.

Let $A_n^{'}$ be the matrix obtained from $A_n$, with first entry of every row deleted. Then the matrix $A_n^{'}$ has n elements of length (n-1), and distance between any two rows of $A_n$ is n/2. The matrix $A_n^{'}$ so obtained is called Hadmard Code of type (n-1, n,n/2). Now we show that it is 2-frameproof code. Since for this code d= $\frac{n}{2}$ , and l=n-1. Therefore d > ( $\frac{l}{2}$ ) i.e. d > (1- $\frac{1}{2}$ )$l$. So by the definition [3] of frame proof code, Hadmard Code with (n-1, n, $\frac{n}{2}$ ) is 2-FP Code.

Example 1.3.1.1: Let us consider a normalized Hadmard Matrix of order 4 given as ;

$$M_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

Then as discussed above, the matrix $A_4^{'}$ will be

$$A_4^{'} = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

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

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

Remark: In [6.], Cohen claims that “Hadmard Codes are $(n-1, n, \frac{n}{2})$are 3-FPC”. But this result is not true always, for this case we present an example.

**Example:** Let H be a Hadmard 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 $$A_8^{'} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

So it is a Hadmard Code H with parameters (7,8,4)as discussed above. Now we show that it is not 3-FPC.Let each codeword of this matrix H is assigned as codewords $c_1, c_2, c_3, c_4, c_5, c_6, c_7$ and $c_8$.if any three users with codewords $c_2, c_6$ and $c_3$ collude, i.e.
W= $\{c_2, c_6, c_3\}$ with
$c_2$ = 1 0 1 0 1 0 1
$c_3$ = 1 0 1 1 0 1 0
$c_6$ = 0 1 1 0 0 1 1

Then by the definition of feasible set defined above ,
F($c_2, c_3, c_6$) = { (0 1 1 1 1 0 0 ), (1 0 1 0 0 0 0),
(0 0 1 0 0 0 1)………….. }

Here in this feasible set , we note that the first codeword we have,is the codeword $c_7$ . Therefore, F $(c_2, c_3, c_6) \cap H \neq \{c_2, c_3, c_6\}$

Hence by the definition [3] of frameproof code, it is not 3-FPC.

## 2. Conclusion

In this paper we show that Hadmard Code in general is not a 3-Frameproof Code. In future we would like to prove the necessary and sufficient conditions for being a Hadmard Code to be 3-Frameproof Code.

## 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 Digital Data” , 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 frame proof 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