International Journal of Science and Research Archive
eISSN: 2582-8185 CODEN (USA): IJSRO2
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Balanced Incomplete Block Design (BIBD) as Traceable Codes

Anu Kathuria [1, *] and Sudhir Batra [2]

[1] *Department of Mathematics, The Technological Institute of Textile and Sciences, Bhiwani, Haryana, India.*
[2] *Department of Mathematics, Deenbandhu Chhotu Ram University of Science and Technology, Murthal Sonepathal, India.*

International Journal of Science and Research Archive, 2023, 08(01), 734–739

Publication history: Received on 02 January 2023; Revised on 09 February 2023; Accepted on 11 February 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.8.1.0165

Abstract

Traceability Codes are Combinatorial Objects introduced by Chor, Fiat and Naor in 1994 [7] to be used in traitor tracing to protect illegal redistribution of Digital Content. Frameproof Codes were given by Boneh and Shaw in 1995 to prevent piracy. Traceable Codes is a strong form of frameproof codes due to efficient traitor tracing algorithm. Study of existence conditions of Balanced Incomplete Block Design in the form of frameproof codes is already available in literature. In the present study we discuss the existence conditions of Balanced Incomplete Block Design in the form of 2-Traceable Codes.

Keywords: Balanced Incomplete Block Design (BIBD); Resolvable Balanced Incomplete Block Design (RBIBD); Traceable Codes

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 [2] 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, b) - 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

$$F(C) = \{ w \in \{0,1\}^v : \{w | u(C) = w^{(u_i)} | u(C) \; for \; all \; w^{(u_i)} \in C \}$$

*Corresponding author: Anu Kathuria

is called feasible set of C. if $u(C)=\emptyset$, 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 codewords they jointly hold. if there is a codeword $w^{(j)} \in F(C)\backslash C$, then user j could be framed in this case.

Definition 1.1 [3]. A (v, b)-code T is called a c-frameproof code if , for every W C 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 at most 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 [3],

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 discussed 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.

2. Traceable Codes

Traceable Codes are the first type of Digital fingerprinting codes defined by Chor, Fiat and Naor [7]in 1994,in order to prevent illegal redistribution of Digital Data. Traceability(TA) codes are a subset of family of Identifiable Parent Property (IPP) Codes. However, their important feature is the algorithm they provide in order to accomplish the identification of pirate. The algorithm based on Traceable Codes is deterministic and is based on the examination of Hamming distance between codewords and words of descendant set. In this section we discuss the definitions and terminologies related to Traceable Codes.

Definition 2.1.[3]. 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

y$\epsilon C_i(C_i$C 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).

Theorem 2.2. [1]. Suppose that C is an (n , $\boldsymbol{q^k}$,d) Code having distance d>(1- $1/\boldsymbol{c^2}$)n. Then C is a c-TA code,

where c = 2,3,4…

Example 2.2.1 . Let C be a code given by

a = 0 1 1

b = 1 0 1

c = 3 2 2

then we show that it is 2-TA Code. if a and b collude and generate a new codeword d = (1,1,1). Then d (a, d)=1

and d (b, d) = 1.So we can observe that distance d is minimum for a and b.

Definition 2.3 . Design [4].

A design is a pair (X,A) such that following properties are satisfied,

- X is a set of elements called points.
- A is a collection of non-empty subsets of X called blocks.if two blocks in a design are identical ,then they are said to be Repeated Blocks .

Definition 2.4 . Balanced Incomplete Block Design (BIBD)[4].

Let v, k and λ be positive integers such that v >k ≥ 2. A (v, k, λ)- BIBD is a design (X,A) such that following properties are satisfied.

- $|X| = v$
- Each block contains exactly k points, and
- Every pair of distinct points is contained in exactly λ blocks.

A BIBD is called an Incomplete Block Design if k (< v).

Example 2.4.1.

A [7 ,3,1]-BIBD is a design with X={1,2,3,4,5,6 ,7} and A= {123, 145, 167, 246, 257,347,356} . Here we observe that each block contains 3 points and every pair of distinct point is contained in 1 block. So as stated above , v=7 and k=3, λ=1.

Theorem 2.5. [4] **.**

In a (v, k, λ)-BIBD , every point occurs in exactly

$r = \frac{\lambda(v-1)}{k-1}$ blocks.

Theorem 2.6 . [4].

A (v, k ,λ)-BIBD has exactly b =$\frac{vr}{k}$ blocks.

Theorem 2.7 . [4].

If a (v, k , λ)-BIBD exists then $v \equiv 1, k \pmod{k^2-k}$

Definition 2.8 . (v, b, r ,k, λ) - BIBD [4].

A Balanced incomplete Block Design with parameters (v, b, r ,k, λ) is defined as an array of v different symbols or elements in b subsets blocks such that every block contains k (< v) different elements ,each element occurs in r blocks and each pair of elements occur in λ blocks.

Definition 2. 9 .Resolvable BIBD [4].

A BIBD is called Resolvable if its b blocks can be separated into r groups or repition of q blocks in such a way that each of the v elements occurs exactly once in each column.

Definition 2.10. Equidistant Code [1].

A code C (n, M, d) is called Equidistant Constant Weight Code if all the codewords are equidistant and consist of same weight.

Theorem 2.11.[1].

An Equidistant code d> $\frac{2n}{3}$ is always a 2-TA code.

in [1], we have already proved that if any code C is equidistant then for distance d of the code i.e. $d > \frac{2n}{3}$,the code C is always 2-TA code. Using this theorem we now define the existence condition of Combinatorial Stuctures Balanced Incomplete Block Design as 2-TA Code in next section.

Definition 2.12.Incidence Matrix[4].

it is often convenient to represent A BIBD by means of an incidence matrix. We give the definition of an Incidence Matrix as, if (X, A) is a design where

X = $\{x_1, x_2, x_3, x_4 \ldots\ldots\ldots x_v\}$ and A = $\{A_1, A_2, A_3, \ldots\ldots A_b\}$.Then the incidence matrix of (X, A) is the(v × b) matrix M = $(m_{i,j})$ defined by the rule.

$m_{i,j} = 1$ if $x_i \in A_j$ and $m_{i,j} = 0$ if x_i *does not belong to* Aj.

Section 3.

Here in this section we discuss the existence conditions of Balanced Incomplete Block Design in form of Traceable Codes. First we mention the existence conditions of Balanced Incomplete Block Designs in form of frameproof codes as available in literature.

Theorem 3.1. [5].

There exist frameproof codes as follows:

- There exists 2- FPC $(v, \frac{v(v-1)}{6})$ for all $v \equiv 1,3 \pmod 6$
- There exists 3- FPC $(v, \frac{v(v-1)}{12})$ for all $v \equiv 1,4 \pmod{12}$
- There exists 4- FPC $(v, \frac{v(v-1)}{20})$ for all $v \equiv 1,5 \pmod{20}$ where 3≤k≤5,

and here FPC defines frameproof code. Here first parameter v represents length of each codeword and second parameter represents number of codewords. Before proving the next result we just represent a result in form of a lemma

Lemma 3.2 .The existence of a- (v, b, r, k, λ) BIBD is equivalent to an Equidistant Code C(n, M, d) with length of the codeword n = b and distance d = v – k.

Proof. Using the definition of incidence matrix discussed above we always find that for an incidence matrix of

(v, b, r, k, λ)-BIBD , every column of M consists of exactly k times 1's. Every row of M consists of r times 1's and two distinct rows of M contain 1's in exactly λ columns . if C is a code consisting of all rows of that incidence matrix as its codewords ,then by the definition of equidistant constant code ,C comes out to be an equidistant code ;where length of every codeword is b = $\frac{vr}{k}$ .The number of codewords here will be v and weight of every codeword is r and distance d between any two codewords is (n –k).

Now we are in a position of deriving the existence conditions of BIBD in form of 2-TA code .

Theorem 3.3

There exist traceable codes as follows **:**

There exists 2- TA code $(v, \frac{v(v-1)}{12})$ for all $v \equiv 1,4 \pmod{12}$, k=4.

There exists 2- TA code $(v, \frac{v(v-1)}{20})$ for all $v \equiv 1,5 \pmod{20}$, k=4.

Proof:

As we have shown in our paper [1] that "An Equidistant code with

d >$\frac{2n}{3}$ is always a 2-TA Code" and here by the definition of BIBD and equidistant constant weight code as discussed above, incidence matrix of a,(v, b, r, k, λ) − BIBD paves to an equidistant code with d= v – k, n=b.

So a (v, b, r, k, λ)- BIBD is 2-TA if

(v –k) >$\frac{2b}{3}$ (i)

Using Theorem 2.6, we have b = $\frac{vr}{k}$.

So (i) becomes 3(v-k) >$\frac{2vr}{k}$ (ii)

By the definition 2.5 discussed above , r = $\frac{\lambda\,(v-1)}{k-1}$ now choosing λ =1 ,we have

r =$\frac{v-1}{k-1}$ and (ii) becomes

3(v-k) > $\frac{2v(v-1)}{k(k-1)}$ (iii)

so 3k(v-k)(k-1) > 2v(v-1)

hence 2(v-1) < 3k(k-1)(v-k) (iv)

by the definition [4],we have k ≥ 2

if k=2 then (iv) becomes

2 v(v-1)< 3.3.2(v-3)

→ v(v-1) < 9v – 27

→ $v^2 - v$ < 9v-27

→ v^2 +27 < 10v (v)

There is no value of v for which (v) will be satisfied.

Therefore k>3.

Case (i)

k=4, and according to Theorem [4]. "if a (v ,k, λ)- BIBD exists then $v \equiv 1, k(mod(k^2$ - k))"

Therefore $v \equiv 1$, 4(mod 12) and by Definition[4], b=$\frac{v(v-1)}{k(k-1)}$.

So , b= $\frac{v(v-1)}{12}$.

Hence the code becomes (v , $\frac{v(v-1)}{12}$), where $v \equiv 1,4(mod\ 12).\ it\ proves\ (i)$

Case(ii)

k=5, so by Theorem 3.1, $v \equiv 1,5$ (mod 20)

and by definition as discussed above ,b=$\frac{v(v-1)}{20}$.

Hence the code is $(v,\frac{v(v-1)}{20})$, where $v \equiv 1,5 \pmod{20}$. It proves (ii)

4. Conclusion

Here in this paper we have defined the existence conditions for combinatorial structures Balanced Incomplete Block Designs in form of 2-TA Codes. In future we wish to discuss the existence conditions of Balanced Incomplete Block Designs in form of 3-TA Codes.

Compliance with ethical standards

Acknowledgments

I am thankful to TITS, BHIWANI for its support and acknowledgment.

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] D. R. Stinson, "Combinatorial Designs: Construction and Analysis", Springer-Verlag, New York ,Berlin ,Heidelberg,2003.

[5] D. R. Stinson ,R.Wei "Combinatorial Properties and Constructions of traceability Schemes and frameproof codes "SIAM Journal of Discrete Mathematics,vol.2,pp.41-53,1998.

[6] Hongxia Jin, Mario Blaum," Combinatorial Properties of Traceability Codes using Error Correcting Codes" IEEE Transformations on Information Theory,vol.53,no.2, February07.

[7] 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.

[8] Anu Kathuria "Combinatorial Properties of Some Fingerprinting Models and Linear Codes" Ph,D. Thesis, Submitted to M.D.U.Rohtak,2013.

[9] Gerard Cohen, S. Encheva," Some new p-array Two Secure frameproof Codes" Applied Mathematical Letters 14(2001);pp.177-282

[10] 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.

[11] 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.

[12] L. R. Virmani," The Theory of Error Correcting Codes", Chapman and Hall/CRC Press