IJSRA

International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

Int. J. Sci. Res. Arch.
IJSRA
International Journal of Science and Research Archive
Research Journal Archive, INDIA

(Review Article)

Check for updates

On frameproof results of Linear Error Correcting codes and Nested BIBDS

Anu Kathuria *

The Technological Institute of Textile and Sciences, Bhiwani-127021, Haryana, India.

International Journal of Science and Research Archive, 2021, 02(02), 274–279

Publication history: Received on 21 May 2021; revised on 26 June 2021; accepted on 28 June 2021

Article DOI: https://doi.org/10.30574/ijsra.2021.2.2.0408

Abstract

In this paper we relate how Equidistant Constant Weight Codes and Different Combinatorial Structures like Resolvable Balanced Incomplete Block Designs (RBIBD) , Nested Balanced Incomplete Block Designs (NBIBD) and Linear Codes are related with each other and then show how these Combinatorial Structures can be used as 2-Traceable (TA) Code.

Keywords: Balanced Incomplete Block Design (BIBD); Resolvable Balanced Incomplete Block Designs (RBIBD); Latin Squares; Linear Codes and Projective Plane

1 Introduction

It is the nature and need of all living creatures to hide some information from others for security ,privacy or due to some other reasons. From the ancient time to the advent of computers various techniques are described to hide the information. Broadly speaking there are three types of information hiding techniques needed in today environment namely – Steganography, Watermarking and Fingerprinting. Fingerprinting is the user unique marking of the data for the purpose of tracing the origin of a discovered , illegal copy of the data. The problem of digital fingerprinting was introduced by Neal R. Wagner [13]in 1983. In the framework of digital content distribution , illegal distribution is a big concern. Therefore ,the digital fingerprinting technique appears as a method to discourage it . For dealing with the problem discussed above four different types of fingerprinting codes are available in literature. These codes are Secure frameproof Codes (SFP), Frameproof (FP) Codes, Identifiable Parent Property (IPP) Codes and Traceable (TA) Codes. Boneh and Shaw introduced the concept of frameproof codes in 1994 and gave the idea of c-secure codes with high probability. They used error correcting Codes to construct c-frameproof codes and obtained sufficient condition for such error correcting codes to be used in tracing the traitor. Combinatorial properties of traceability schemes and frameproof codes have been studied by Stinson and Wei[4,5].Sufficient conditions for an equidistant code to be an IPP Code have been derived in [10].In [1] we have derived the necessary and sufficientconditions for equidistant constant weight codes to be 2-TA code .Here in this paper we discuss the definitions and terminologies that we will be using in proving our results.In Section 3,we prove our result and relate Combinatorial Structures Resolvable BIBDS, Nested BIBDS and Linear Error Correcting Codes.

2 Preliminaries

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

- 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 Care called codewords oflength n.

*Corresponding author: Anu Kathuria

- Let a and b be two codewords , then the hamming distance between a and b i.e. 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 , b ϵ C }.
- 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…..
- A subspace C of F_q^n is called a linear code over $F_{q.}$The dimension of the code is defined as the dimension of the subspace. A linear code with length n, dimension k and minimum distance d is denoted as [n, k, d] code.
- A linear code C [n ,k, d] is a Maximium Distance Separable code if d = n – k + 1
- A code C with same distance for every pair of codewords is called equidistant code and if all the codewords carry same weight then it is called Equidistant Constant Weight Code.

2.2 Here we define some terms related to fingerprinting codes

- **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.
- **Coalition**: it means two or more users meet for the purpose of creating an illegal copy of a digital object (see Marking Assumption also) by comparing their copies. A member of the coalition is called a pirate.
- **Descendant Set**: For any two words a = {$a_1, a_{2,} \ldots\ldots a_n$} and b={$b_1$,$b_2 \ldots\ldots b_n$} 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……
- **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,….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.
- **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 yϵC_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).
- **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 onlycodewords 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 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.

- **Linear Code :** A Linear code over GF(q) is just a subspace of V (n , q) **, f**or some positive integer n. Thus a subset C of V (n , q) is a Linear code if and only if
  (i) u + v ∈ C for all u and v in C and
  (ii) au ∈ C for all u in C ,a ∈ GF(q)

*2.1.1 Theorem 2.2.1[*4]

Suppose that C is an (n ,q^k ,d) code having distance ; d>(1- 1/c^2)n. Then C is a c-TA code, where c = 2,3,4…….

In Section 3, we show that how Equidistant Constant Weight Codes and Resolvable BIBDS are related with each other and how these can be used as 2-TA Codes .

3 Resolvable BIBD as 2-TA Code

In this section we show that how Resolvable BIBD can prove to be 2-TA code. Let us recall some basic definitions.

- **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.

- $(a)|X|$ = v
- (b) Each block contains exactly k points, and
- (c) Every pair of distinct points is contained in exactlyλ blocks.

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

Example**:** 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.

- **Resolvable BIBD**: A BIBD is called resolvable if its b blocks can be partitioned into r groups or repetition of q blocks in such a way that each of the v elements occurs once in each column.

Definition 3.1 (Plotkin Bound [12]) : Let C be a Code of length n, size N and minimum distance d over Q with m elements then d≤$\frac{nN(m-1)}{(N-1)m}$.

If d =$\frac{nN(m-1)}{(N-1)m}$then C is said to be optimal code also.

Lemma [1] A Linear MDS Code C [q+1, 2, q]is an Equidistant Constant Weight Code. Moreover C is optimal also.

Theorem.2: The existence of Optimal Equidistant (n, M, d) Codes and Resolvable BIBDs (v= qk , b, k ,r, λ) are equivalent to one another and their parameters are connected by the conditions v = M,b = nq , k = q ,r = n, λ = n-d.

Theorem 3: The existence of a linear MDS Code satisfying [n=q+1, k=2, d = q] and Resolvable BIBD

(v=qk, b, k, r, λ) are equivalent to one another and their parameters are connected by the conditions

v =q^2,b =(q+1)q, k = q, r = q+1, λ = 1.

Proof: Since as we know that number of codewords in Linear MDS code C satisfying

[n = q+1, k=2, d=q] are q^2. Therefore by using Theorem 2 and above Lemma proved by us earlier in our reference paper [1] we can easily prove this result. Here we present an example in this contest.

Example : Linear MDS Code over [4,2,3] over F = {0,1,2} is equivalent to (9,12,3,4,1)- RBIBD given by

C **=**{ 0000, 1111, 0222, 1012, 1201, 2021, 2102, 2210 } by the definition 2.2.1[4], here we find that distance d of the code is 3 and it also satisfies the condition $d > \left(1-\frac{1}{4}\right)n$. So it is 2-TA Code. In the same way RBIBD with the parameters of (v, b, k, r , λ)i. e. using (9,12,3,4,1) such values that example is also a 2-TA code.

Example : Here we quote an example in this context.

Reed Solomon Code [5, 2, 4] over F = {0, 1, a, a^2} is equivalent to (16,20,4,5,1)- RBIBD given by

Table 1 Reed Solomon Code

0	0	0	0	0
0	1	a	a	1
0	a	a^2	a^2	a
0	a^2	1	1	a^2
1	a	a	1	0
1	a^2	0	a^2	1
1	0	1	a	a
1	1	a^2	0	a^2
a	a^2	a^2	a	0
a	a	1	0	1
a	1	0	1	a
a	0	a	a^2	a^2
a^2	1	1	a^2	0
a^2	0	a^2	1	1
a^2	a^2	a	0	a
a^2	a	0	a	a^2

Since n=5 and d=4. So $d > (1-\frac{1}{4})n$. Therefore by definition 2.2.1.this (16, 20, 4, 5 ,1)-RBIBD is 2-TA Code. So here we conclude that as linear MDS codes can be used as 2- TA codes in the same way Resolvable BIBDS can be used as 2-TA codes. These codes even prove to be good optimal codes also.

4 Nested Balanced Incomplete Block Designs as 2-TA Code

Definition 4.1[3]: Let v, k_1 , k_2 , λ_1 ,λ_2 be positive integers such that v $\geq k_1 > 1$ and $k_2 > 1$ divides k_1 . A (v,k_1,k_2,λ_1 ,λ_2) *nested* BIB design is a triple (V, $B_{1,}$, B_2) where

- V is a set of elements called points.
- $B_{1,}$ and B_2 are collections of k_1- subsets (called superblocks)andk_2-subsets(called subblocks) of V respectively, where each superblock of $B_{1,}$*is* partitioned into $\frac{k_1}{k_2}$ subblocks having k_2 elements each such that the resulting collection $B_{1,}$ of subblocks coincides with the collection B_2.
- For every pair of distinct points x,y $\in V$, there are λ_1 superblocks and λ_2 subblocks containing x and y respectively.

Theorem 4: The existence of a (v,k_1, k_2,λ_1 ,λ_2)-nested BIBD is equivalent to an equidistant code (b_1,v,2r-λ_1- λ_2 ; 1+ $\frac{k_1}{k_2}$) code where $\frac{k_2}{k_1} = \frac{b_2}{b_1}$.

The following seven codewords of Nested BIBD form an equidistant (21, 7, 16 ,3) code C with n=21,M=7,d=16,q=3

Table 2 Nested BIBD with parameters (21,7,16,3)

1	0	0	2	0	2	1	1	0	2	0	0	2	1	1	0	0	2	0	1	2
1	1	0	0	2	0	2	1	1	0	2	0	0	2	2	1	0	0	2	0	1
2	1	1	0	0	2	0	2	1	1	0	2	0	0	1	2	1	0	0	2	0
0	2	1	1	0	0	2	0	2	1	1	0	2	0	0	1	0	1	1	0	2
2	0	2	1	1	0	0	0	0	2	1	1	0	2	2	0	1	2	1	0	0
0	2	0	2	1	1	0	2	0	0	2	1	1	0	0	2	0	1	2	1	0
0	0	2	0	2	1	1	0	2	0	0	2	1	1	0	0	2	0	1	2	1

Since for code C, d =16 and n =21 Therefore d > (1-1/4) n (m=2).So by the above theorem 2 discussed above ,this RBIBD is equivalent to an equidistant constant weight code and in our paper [1] we have shown that an equidistant constant weight code C is 2-TA if $d > 2n/3$. So for this result the above example of RBIBD is also a 2-TA code.

5 Conclusion

Here in the present study I have shown that Algebraic Combinatorial Structures Nested BIBDS and Resolvable BIBDS are related with linear error correcting Codes and how such combinatorial structures can also be used as under the same conditions can be used as 2-TA codes. In future I wish to derive the existence conditions of some infinite families of other Combinatorial Structures that also can be used as 2-Traceable(TA) Code and 3- Traceable Code.

Compliance with ethical standards

Acknowledgments

I wish to thank the referees for their valuable comments that help in improving the quality of the paper.

References

[1] Anu Kathuria, Sudhir Batra and S.K. Arora ” On traceabilty property of equidistant codes” Discrete Mathematics, Elsevier,vol.340,issue4,April2017,pg.713-721

[2] D. Boneh and J. Shaw, ”Collusion –Secure fingerprintingfor Digital Data” ,IEEE Transactions on Information Theory,vol.44, pp. 1897-1905, 1998.

[3] D. Boneh and J. Shaw,” Collusion –Securefingerprintingfor DigitalData”, 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] HongxiaJin, Mario Blaum,” Combinatorial Properties of Traceability Codesusing 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, SpringerVerlag, vol. 839, pp. 257-270 ,1994.

[8] Gerard Cohen, Encheva Sylvia “Frameproof Codes against coalition of pirates” Theoretical Computer Science, vol.2 73(2002), pp.295-304.

[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

[13] K. Sinha, Z. Wang, D. Wu ,”Good Equidistant Codes constructed from certain Combinatorial Designs ”Discrete Mathematics ,vol.308(2008) pp.4205-4201

[14] N. Wagner ,”Fingerprinting Technique “, in proceedings 1983, IEEE Symposium on Security and privacy ,pp.18-22,April 1983.