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

On Traceability Property of Linear Codes and Resolvable BIBDS

Anu Kathuria[1], Sudhir Batra[2]

The Technological Institute of Textile and Sciences, Bhiwani-127021, Haryana, India
anu_sept24[at]rediffmail.com
Department of Mathematics, DCR University of Technology and Sciences, Murthal, Haryana, India

Abstract: ***Traceability Codes are Combinatorial Objects introduced by Chor, Fiat and Naor in 1994 [7] to be used in traitor tracing to protect Digital Content. Frameproof Codes were given by Boneh and Shaw in 1994 to prevent privacy and gave the idea of c-secure codes with ε-error. Traceable Codes is a strong form of Frameproof Codes. Balanced Incomplete Block Design Codes in form of frameproof codes are already available in literature [4]. Here in this paper we define how Equidistant Constant Weight Codes and Different Combinatorial Structures like Resolvable Balanced Incomplete Block Designs are related with each other and then represent the conditions for being these Algebraic Structures to be 2-Traceable Code.***

Keywords: Resolvable Balanced Incomplete Block Designs (RBIBD), Latin Squares and Projective Plane

1. Introduction

Chor, Fiat and Naor introduced the concept of Traitor tracing as a means to limit piracy. Traitor tracing schemes may prove quite useful in protecting copyrighted digital data. When a pirated copy created by a group of authorized users of the copyrighted data is traced, traitor tracing schemes allow to trace it back to at least one producer of it. In recent years several codes have been studied for the purpose of their usefulness in traceability schemes. In general these codes are called fingerprinting codes. The weak form of these codes called frameproof codes were introduced by Boneh and Shaw [2]. Strong form of codes called Identifiable Parent Property (IPP) Codes have been introduced by Hollman and Van Lint [10]. Other form of codes called traceability codes were introduced by Chor, Fiat and Naor [7]in 1994. TA codes are stronger than IPP codes and is a subclass of IPP codes and generally have efficient traitor tracing algorithm. IPP codes on the other hand are capable of identifying traitors requiring less restrictive conditions than TA codes at the expense of having not efficient traitor tracing algorithm. 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 sufficient conditions for equidistant constant weight codes to be 2-TA code. Here in Section 2 we discuss the definitions and terminologies that we will be using in proving our results. In Section 3, we prove our result and show the relation between Linear MDS codes and Resolvable BIBDS.

2. Preliminaries

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

2.1 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 Care 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…. .

(iv) 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.

(v) A linear code C [n, k, d]is a Maximum Distance Separable code if d=n-k+1

(vi) 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 Now let us define some terms related to fingerprinting codes

1) 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 i^{th} position of each word x ϵ X is occupied with the same alphabet, otherwise the position is detectable.
2) 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.
3) 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 $\epsilon\, Q^n \mid x_i \epsilon \{ a_i, b_i \}$, i=1, 2, 3…n}The above definition of descendant set can be naturally extended to any finite number of words a, b, c……

4) 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.
5) Traceable Code: For x, y $\epsilon\, Q^n$; define I (x, y)={i: $x_i = y_i$ }. C is c-TA code provided that for all I and for all x $\epsilon\, desc_c$ ($C_{i)}$) there is atleast one codeword yϵC_i ($C_i \subset$ 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).
6) Frameproof Code: A (v, b)-code T is called a c-frameproof code if, for every W $\subset$ 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: 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.

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.

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.
(i) 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 exactly λ 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.

(ii)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 $\leq \frac{nN\ (m-1)}{(N-1)m}$.

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.

Proof: As the number of codewords of weight q in C is q^2-1. Since the code C is linear with size q^2, each nonzero codeword of C must be of weight q and hence is an equidistant code. Further minimum distance of the code meets the Plotkin Bound [12], i.e. d = q = $\frac{(q+1)\ (q-1)q^2}{(q^2-1)q}$ and hence is optimal also.

Theorem 3.2 [13]: The 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 = n. q, k = q, r = n, λ = n-d.

Theorem 3.3: 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 number of code words in Linear MDS Code C satisfying

[n = q+1, k=2, d = q] are q^2. Therefore by using Theorem 3.2 and above Lemma proved by us earlier can complete this result. Here we present an example in this context.

Example 3.3.1: 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 distance d is 3 and it satisfies the condition $d > \left(1 - \frac{1}{4}\right) n$. So it is 2-TA Code. In the same way RBIBD (9, 12, 3, 4, 1) is 2-TA code.

4. Conclusion

Here in that paper we mention some infinite families of equidistant codes which will be used as 2-TA codes. It will be interesting to obtain some other infinite families of equidistant codes for using them as 2-TA codes.

References

[1] Anu Kathuria, Sudhir Batra and S. K. Arora " On traceabilty property of equidistant codes" Discrete Mathematics, Elsevier, vol.340, issue4, 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 frame proof 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, February 07.
[7] B. Chor, A. Fiat and M. Naor, "Tracing Traitors", in Advances in Cryptology - CRYPTO 94 (Lecture Notes in Computer Science)B erlin, Germany, Springer Verlag, vol. 839, pp. 257-270, 1994.
[8] Gerard Cohen, Encheva Sylvia "Frameproof Codes against coalition of pirates" Theoretical Computer Science, vol.273 (2002), pp.295-304.
[9] Gerard Cohen, S. Encheva, " Some new p-array Two Secure frame proof 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 frame proof 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