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

(REVIEW ARTICLE)

Check for updates

On Algebraic Conditions of Equidistant 2-TA Codes

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

[1] *The Technological Institute of Textile and Sciences, Bhiwani, India.*
[2] *Department of Mathematics, DCRUST, Murthal, India.*

International Journal of Science and Research Archive, 2023, 08(02), 575–588

Publication history: Received on 02 March 2023; Revised on 09 April 2023; Accepted on 12 April 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.8.2.0295

Abstract

Necessary and Sufficient Conditions for an Equidistant Code to be 2-TA code have been obtained in [1,2]. In the present paper we revisit these using pictorial approach. Further we discuss these conditions again under which an Equidistant Code is not a 2-TA Code.

Keywords: Traceable Codes; Equidistant Codes; Combinatorics; Frameproof Codes; Mathematics

1. Introduction

The problem of Digital Fingerprinting was introduced by Neal R. Wagner [3] in 1983. In the framework of digital content distribution, illegal redistribution is a major concern. Therefore, the digital fingerprinting technique appears as a method to discourage it. In this case, the distributor embeds in the digital content, using a watermarking algorithm, a unique piece of information for each user. If the content is illegally redistributed, the fingerprint can be extracted and dishonest user can be identified. 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 [4]. Strong form of codes, called identifiable parent property (IPP) codes have been introduced by Hollman ,Van Lint and Linnartz [8].Other form of codes ,called traceability codes were introduced by Chor, Fiat and Naor in [7]. Traceable (TA) codes are stronger than IPP codes and are 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 Traceable (TA) codes at the expense of not having efficient traitor tracing algorithm. Combinatorial properties of traceability schemes and frameproof codes have been studied by Staddon, Stinson and Wei in [9]. Sufficient conditions for an equidistant code to be an IPP code have been derived in [8]. Some constructions of equidistant frameproof codes have been suggested in [9]. Necessary and sufficient conditions for an equidistant code to be 2-TA are discussed by us in [1]. In the present paper in Section 3, we give the detailed proof of the Mathematical conditions using pictorial approach under which an equidistant code can be 2-TA code and those algebraic conditions for which an equidistant code cannot be 2-TA code.

The following section is devoted to some preliminaries required for the discussion in the subsequent sections.

2. Some Preliminaries

Throughout the paper, we will follow the terminology and assumptions made in [1, 2] and these are reproduced below in 2.1 and 2.2. Here F_q denotes a finite field with q elements.

*Corresponding author: Anu Kathuria

Copyright © 2023 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution Liscense 4.0.

2.1 First 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 C are called codewords oflength$n$.
- Let a and b be two codewords ,then the hamming distance between a and b is $d(a,b)$, the number of coordinates in which they differ and the number of nonzero coordinates of a word c is called the weight of c. The minimum distanced of C is $d = min.\{d(a,b)|\ a,b\epsilon C\}$.
- $I(x,y) = \{i: x_i = y_i\} for x = \{x_1, x_2..x_n\}, y = \{y_{1,} y_2..y_n\}\epsilon Q^n$ .Similarly we can define $I(x,y,z..)$ for any number of words x,y,z..
- A code C with same distance between every pair of codewords is called an equidistant code. If all the codewords of code C carry same weight then code C is called constant weight code. A code C with both of these properties is known as equidistant constant weight code

2.2 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 $i \in Q^n$ is undetectable for X if ith position of each word $x\epsilon$ 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 = $\{a_1, a_{2,} \ldots\ldots a_n\}$ and

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

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

  y$\epsilon C_i (C_i$C C) ; $|(x,y)|>|(x,z)| for any y z \epsilon C / C_{i.}$ The condition in terms of distance is equivalent to$d(x,y) < d(x,z)$.

  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. Now let a and b collude and generate a new codeword$d = (1,1,1)$.

Here distance $d\ (a\ , d) = 1, d\ (b, d\ ) = 1$ and$d\ (c, d\ ) = 3$. So we can observe that distance $d$is minimum for a and b. Therefore C is 2-TA code.

Theorem 2.3.1: Sufficient Condition [9]

Suppose that C is an $(n, M, d)_q$ - code having minimum distance$d > (1 - 1/m^2)n$. Then C is a c-TA Code

(c = 2,3,4..)

Theorem 2.3.2: Necessary and Sufficient Condition [6]

Let C be a linear $[n, k, d]$ MDS code over a finite field $GF(q)$ such that $n \leq q + 1$. Then for $m \geq 2$, C is an

m- traceability code if and only if $d > (1 - 1/m^2)n$.

Section 3

In this section we discuss proof of the Mathematical conditions for which an equidistant code can be used as a 2-TA code and we also discuss those algebraic conditions for which an equidistant code cannot be 2-TA code.

Remark

In view of Marking Assumption discussed above**,** we see that the detected positions, where the colluders can make changes in their respected codewords to get a collusion word, are independent of the undetected positions, where the changes are not possible. So, without loss of generality (w.l.o.g) we will pictorially represent the undetected positions (matching positions) say, s in number of two codewords by some s consecutive coordinate positions of the respective coordinates in proving our next theorems. It is quite obvious that matching positions of any two codewords need not be consecutive actually. The following results have already been obtained in [1, 2]. We discuss the proofs of these in a detailed manner using a pictorial approach.

Theorem 3.1[1]

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

Proof. Let '*C*' be an equidistant code of length *n* with distance $d\left(> \frac{2n}{3}\right)$. Let *a* and *b* be any two codewords of *C*. Let'*s*' be the number of positions in which codewords *a* and *b* match. Then *d* = *n* – *s*.

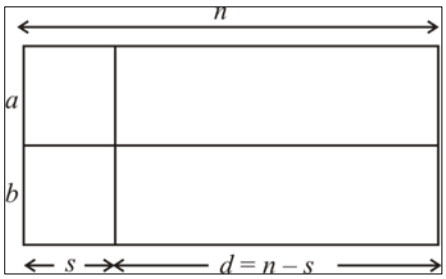

Figure 1 Matching of *a* and *b*

Let *c* denote the codeword obtained by collusion of *a* and *b*. Since the word *c* is obtained by making the changes in

'*n* – *s*' coordinates, where *a* and *b* differ, so w.l.o.g. we can suppose that the first *s* coordinates of *a* and *b* are same as shown in the Fig. 1.

Let *x* be any codeword of *C* other than *a* and *b*. To show that *C* is 2-TA, we have to show that there is no codeword *x* in *C* such that $d(x, c) < d(a, c)$ or $d(x, c) < d(b, c)$. We now consider the following three cases depending on how the *s* matching positions of *x* with the codewords *a* and *b* are situated among the *n* coordinates relative to the *s* matching coordinates of *a* and *b*.

Case I.

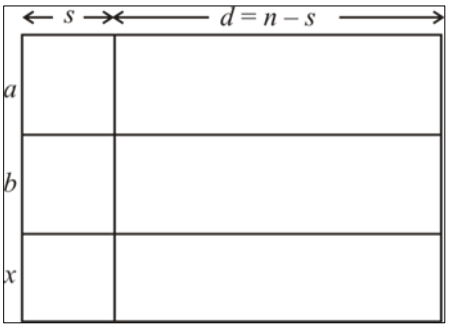

Figure 2 Matching of *a*, *b* and *x*

Suppose that the codewords a and *b* match with *x* at first *s* coordinates as shown in Fig. 2. Now suppose a word *c* is obtained by retaining some k_1 coordinates of *a* and some k_2 coordinates of *b* among (*n* – *s*) nonmatching coordinates of *a* and *b*. Obviously, the first a matching coordinates of *a* and *b* are the first *s* coordinates of *c*.

Observe that $k_1 > 0$ and $k_2 > 0$. For if $k_1 = 0$ then *c* = *b*, which is not possible. Similarly if $k_2 = 0$, then *c* = *a*, which is again not possible. Therefore $k_1, k_2 > 0$.

Further $k_1 + k_2 = n - s$ implies that $k_1, k_2 < n - s$. Since $d(x, a) = n - s = d(x, b)$ and *c* is obtained using the symbols of *a* and *b*. Therefore *d* (*x*, c*) = n – s.*

Now observe that $d(a, c) = n - s - k_1, d(b, c) = n - s - k_2$. This gives us that $d(a, c) < d(x, c)$ and $d(b, c) < d(x, c)$ for all $x \neq a, b$ in *C*.

First, let, $k_1 < k_2$ then $d(a, c) < d(b, c)$ and this implies that colluder *a* is the unique codeword at the smallest distance from the collusion word (pirated word) *c*. Hence *a* will be traced.

Similarly if $k_2 > k_1$, then $d(b, c) < d(x, c)$ and hence the pirate *b* will be traced. Finally, in case $k_1 = k_2$ (This case is possible only when $k_1 + k_2 = n - s$ is even) we have $d(a, c) = d(b, c)$ and thus we can conclude that both *a* and *b* are pirates.

Case II

In this case, we suppose that the codewords *a* and *b* match with *x* at first *l* (> 0) positions such that *l* (<*s*) as depicted in the Figure 3.

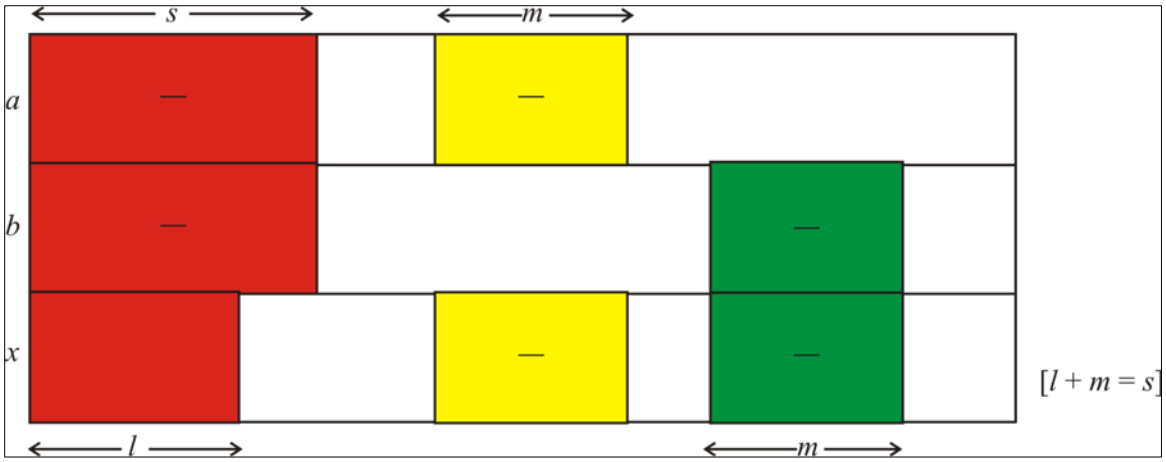

Figure 3 Matching of *a* , *b* and *x* at *l* positions, l < s

Further, we suppose that '*a*' matches with *x* at some *m* positions and *b* matches with *x* again at some *m* different positions as shown in the Figure 3.3, since the code *C* is equidistant, we have *l* + *m* = *s*. Further since $d > \frac{2n}{3}$ i.e.

$$s < \frac{n}{3} \text{ and so } n-3s>0.$$

Now *l*> 0 and *l* + *m* = *s*, so *n* – *s* – 2*m*> 0.

Therefore, there are some corresponding coordinate positions other than *s* matching coordinates of *a* and *b*, left in *a* and *b* which do not match with *x* [see Diagram for clarity].

Now, let a collusion word *c* is obtained by

- (i) Retaining symbols at some m_1 coordinates out of m coordinates shown by yellow color of codeword 'a' where $0 \le m_1 \le m$.
- (ii) Retaining the symbols at some m_2 coordinates out of m coordinates shown by green color of codeword b where $0 \le m_2 \le m$.
- (iii) Retaining the symbols at some k_1 coordinates out of (n – s – m) coordinates i.e. coordinates in unshaded portion of the codeword a.
- (iv)Retaining the symbols at some k_2 coordinates out of (n – s – m) coordinates i.e. Unshaded position of codeword b.

$$\text{then } m_1+m_2+k_1+k_2=n-s.$$

Further, we have

$$d(a,c)=n-s-(m_1+k_1)$$

$$d(b,c)=n-s-(m_2+k_2)$$

$$d(x,c)=n-l-m_1-m_2$$

Since $a \neq c$ and $b \neq c$, $m_1+k_1>0$ and $m_2+k_2>0$. Further since *n* – *s* – 2*m*> 0, so $k_1>0$ or $k_2>0$, i.e. even in case $m_1=m$ and $m_2=m$, we have $k_1>0$ or $k_2>0$. Now there are three cases to be discussed as follows:

- (i) $k_1,k_2>0, 0 \le m_1 \le m$ and $0 \le m_2 \le m$

In this case

$$d(a,c)=n-l-m_1-m_2-m_1-k_1,\ d(b,c)=n-l-m_1-m_2-m_2-k_2 \text{ and } d(x,c)=n-l-m_1-m_2.$$

Then $d(a,c)<d(x,c)$ and $d(b,c)<d(x,c)$. Therefore *a* and *b* will be traced as pirate.

- (ii)$k_1=0$ then as discussed above. Therefore we have $0\le m_1\le m$ and $0\le m_2\le m$

In this case,

$$d(a,c)=n-l-m_1-m_2-m$$

$$d(b,c)=n-l-m_1-m_2-m_2-k_2$$

$$d(x,c)=n-l-m_1-m_2$$

So we have $d(a,c)<d(x,c)$ and $d(b,c)<d(x,c)$. However $d(a,c)<d(b,c)$, $d(b,c)<d(a,c)$ or $d(a,c)=d(b,c)$ according to $m_1>m_2+k_2$, $m_1<m_2+k_2$ 'or' $m_1=m_2+k_2$.

- (iii) $k_2=0$ then as discussed above $k_1>0, m_2>0$ Therefore we have, $k_1=0, k_2=0$, and $0\le m_2\le m$. Now as discussed in *case (II),* we have a or b will be traced as pirate.

Case III

Let *x* be the codeword such that it matches at *s* coordinates with codewords *a* and *b* such that *s* coordinate positions common to *a* and *b*, *a* and *x*, *b* and *x* are all non-intersecting in pairs, as shown in Fig. 4.

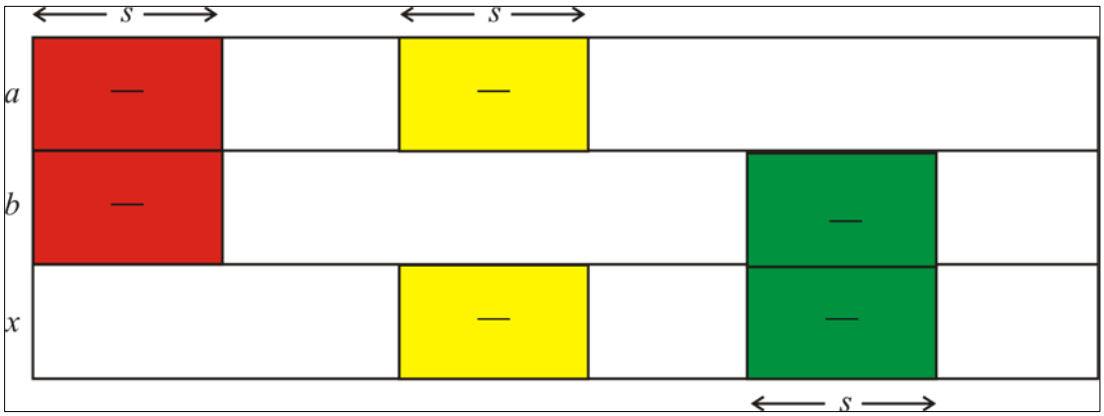

Figure 4 Matching of *a* and *x*, *b* and *x* at *s* positions

$$\text{If } s<\frac{n}{3}, \text{ then } n-3s>0$$

$$\text{i.e. } (n-s)-2s>0$$

Therefore there are some corresponding coordinate positions other than *s* matching coordinates of *a* and *b*, left in *a* and *b* which do not match with *x* (see figure for clarity).

Now let a collusion word *c* is obtained by

- (i) Retaining the symbols at some s_1 coordinates out of s coordinates shown by yellow color of codeword a, where $0 \leq s_1 \leq s$
- (ii)Retaining the symbols at some s_2 coordinates out of s coordinates shown by green color of codeword b,where $0 \leq s_2 \leq s$.
- (iii) Retaining the symbols at some k_1 coordinates out of n – s coordinates, i.e. unshaded portion of codeword 'b'.

Then $.s_1+s_2+k_1+k_2= n - s$

Further we have

$$d(a,c) = n - s - (s_1 + k_1)$$

$$d(b,c) = n - s - (s_2 + k_2)$$

and $d(x,c) = n - (s_1 + s_2)$

Now as discussed in case *II*, $d(a,c) < d(x,c)$ and $d(b,c) < d(x,c)$ and therefore *a* or *b* will be traced as pirates.

Now, we will provide the conditions such that *a* code '*C*' with $d < \frac{2n}{3}$ can also be a 2-TA code, i.e., the condition $d > \frac{2n}{3}$ is the sufficient condition only.

Theorem 3.2

Let *C* be an equidistant code of length *n* with $d = \frac{2n}{3}$. Let *s* denote the number of coordinate points where any two codewords of *C* match. Further, let for any $x \in C$, a, b and *x* match in *l* coordinate positions. Then

- (i) If l = 0 for some$x \in C$, then C is not a 2-TA code.
- (ii)If l > 0 for all x and all the pairs $a, b \in C$, then C is a 2-TA code.

Proof: (i) Since $d = \frac{2n}{3}$, so $s = \frac{n}{3}$. Let there exist a $x \in C$ such that *l* = 0. Then all matching coordinates i.e. $s = \frac{n}{3}$, between *a* and *b*, *a* and *x*, *b* and *x* are non-intersecting. Pictorially, we can represent this situation as follows, in Fig.5.

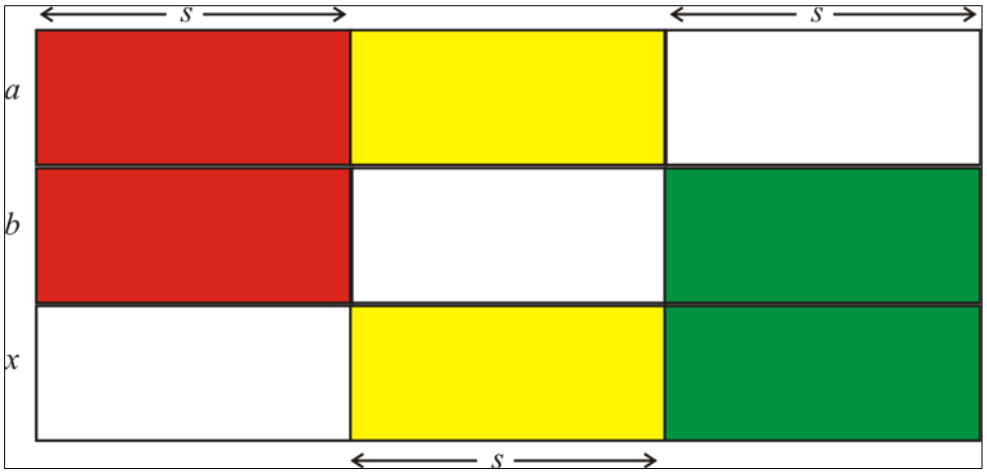

Figure 5 Matching of *a and b* ; *a and x* ; *b and x at s positions*

Let '*c*' be a word obtained by the collusion of codewords *a* and *b* by retaining the *s* coordinates of *a* shaded by yellow color and retaining the *s* coordinates of *b* shaded by yellow color and retaining the *s* coordinates of *b* represented by green colour out of $n - s$ non matching coordinates of *a* and *b*. Then $d(a,c) = n - s, d(b,c) = n - s$ and $d(x,c) = n - s$ .In that case even codeword *x* will be traced. So the code *C* is not 2-TA code. This proves (i).

(ii) Let *l*> 0, for all *x* and all the pairs $a, b \in C$. Then $(n-s)-(s-l)-(s-l) > 0$ i.e. $n-3s+2l > 0$. This situation is pictorially represented as

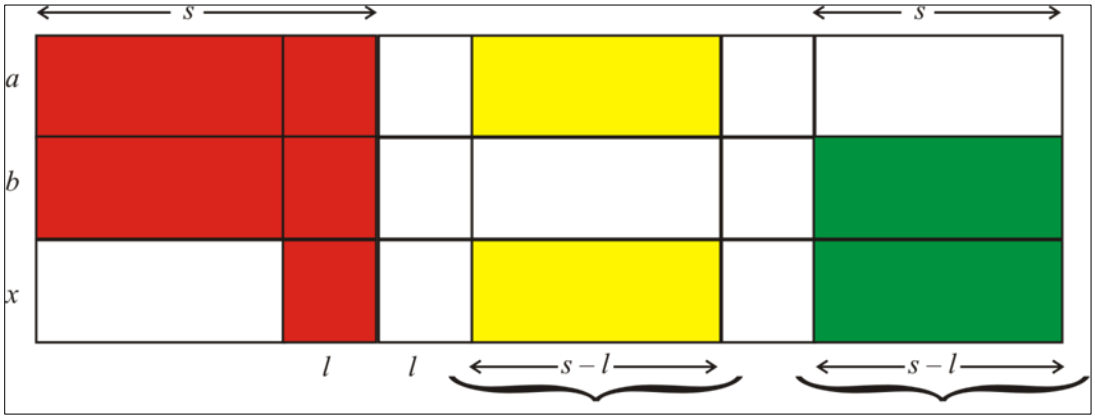

Figure 6 Matching of *a, b andx* ; *a and x*; *b and x with* $n - 3s + 2l > 0$

This case is analogous to the case *II* already discussed in Theorem 3.1. Therefore in this case *C* is a 2-TA code.

Theorem 3.3

Let *C* be an equidistant code of length *n* with $d < \frac{2n}{3}$. Let *s* denote the number of coordinate positions where any two codewords match. Then for any $x \in C$, *a*, *b* and *x* match in *l* coordinate positions, where $0 < l \le s$. Further,

(i) if there is some $x \in C$ such that $n-3s+2l = 0$, then the code *C* is not a 2-TA code.

(ii) if $(n-3s+2l) > 0$ for all *x*, and all the pairs $a, b \in C$, then *C* is a 2-TA code.

Proof. (i) Since $d < \frac{2n}{3}$, so $s > \frac{n}{3}$ and therefore $n - 3s < 0$. Since any two codewords match in exactly *s* coordinate positions, therefore for any $x \in C$ we can't have the case in which *s* matching positions of *a* and *b*, *a* and *x*, *b* and *x* are non-intersecting. Hence for any $x \in C$, all three *a*, *b* and *x* match in *l* positions where $0 < l \leq s$ (Here note that *l*> 0). We now discuss two cases:

(i) if there is some $x \in C$ such that $n - 3s + 2l = 0$

$\Rightarrow n - s = (s - l) + (s - l)$. This situation is pictorially represented as:

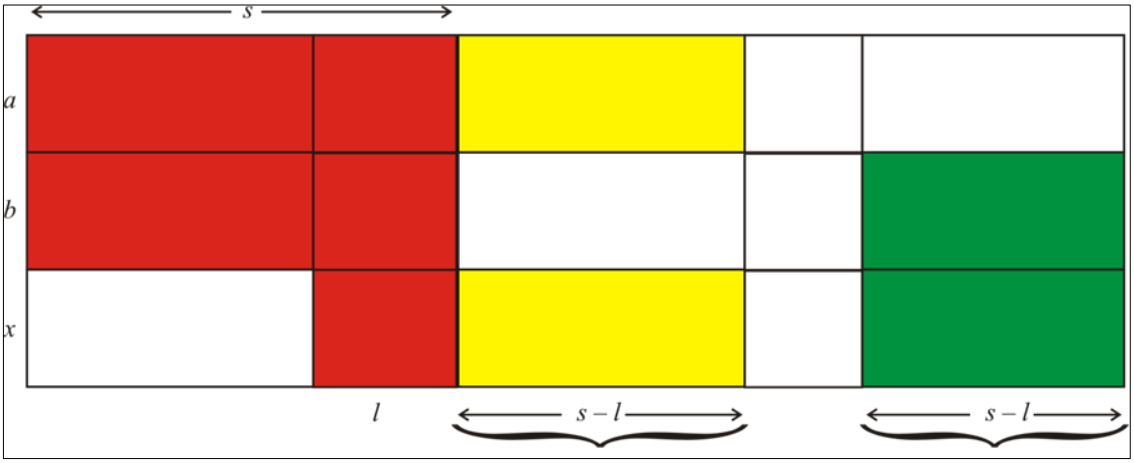

Figure 7 Matching of a, b and x ; a and x; b and x with $n - 3s + 2l = 0$

This case is analogous to the case (i) discussed in Theorem 3.2. This proves (i).

(ii) If for any $x \in C$ and all the pairs $a, b \in C$ we have $n - 3s + 2l > 0$. This situation is pictorially represented as:

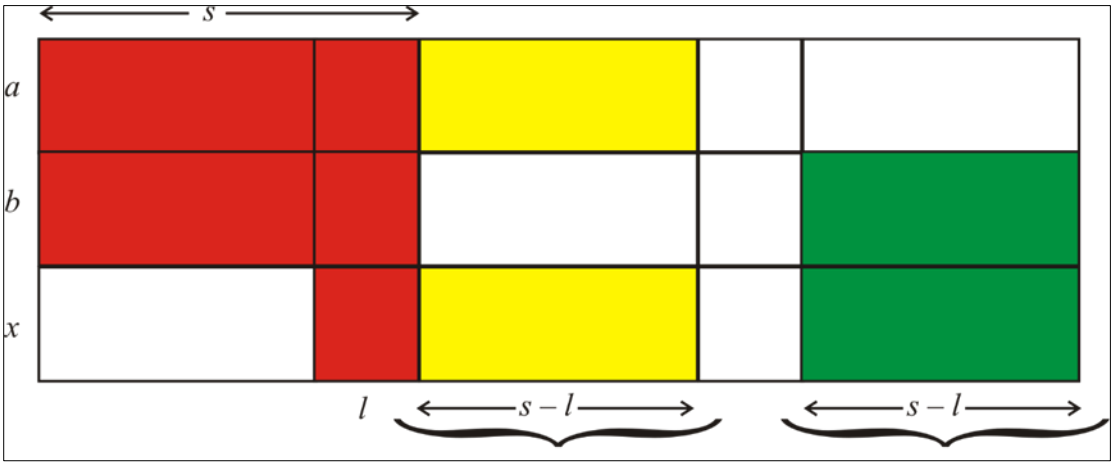

Figure 8 Matching of a, b and x ; a and x; b and x $n - 3s + 2l > 0$

This case is analogous to the case (ii) already discussed in Theorem 3.2. Therefore in this case *C* is a 2-TA code. This proves (ii).

Now we give various examples corresponding to the Theorems discussed above.

Example 3.2.1: Let *C* be a code of length *n* = 6, *d* = 4 given by

$$\begin{aligned} c_1 &= 0\ 0\ 1\ 1\ 1\ 1 \\ c_2 &= 0\ 1\ 0\ 1\ 2\ 2 \\ c_3 &= 0\ 1\ 2\ 2\ 0\ 1 \\ c_4 &= 1\ 0\ 0\ 2\ 2\ 1 \\ c_5 &= 1\ 0\ 2\ 1\ 0\ 2 \\ c_6 &= 2\ 2\ 0\ 1\ 0\ 1 \end{aligned}$$

It is equidistant constant weight code with distance 4. The above code *C* satisfies the condition $d = \frac{2n}{3}$. Here we show that this code *C* is not a 2-TA Code. If we take first and third codeword and they generate a new codeword

(0 0 2 1 0 1), using the codewords

0 0 1 1 1 1

0 1 2 2 0 1

Then in this case, $d(c_1, c) = 2$, $d(c_2, c) = 4$, $d(c_3, c) = 2$, $d(c_4, c) = 4$, $d(c_5, c) = 2$, $d(c_6, c) = 3$. So in that case even c_5 will be traced, since distance *d* is minimum for c_5.

It is easy to notice that the above graph corresponds to case (i) of Theorem 3.2. So the above code is not 2-TA code.

Example 3.3.1: Now we quote an example of a code *C* with distance $d < \frac{2n}{3}$ given by,

n = 8 and *d* = 5, with

a_1 = 0 2 0 1 3 2 0 3

a_2 = 0 0 2 1 0 3 2 3

a_3 = 0 0 0 1 1 1 1 1

a_4 = 1 0 0 0 3 1 2 3

Since for any pair of two codewords (a_i, a_j) of code *C* there are $4C_2 = 6$ pairs. Here, we show the collusion of each pair (a_i, a_j) one by one and verify that the code *C* is 2-TA code. Let us discuss each case one by one.

(i) if $a_1 = 0\,2\,0\,1\,3\,2\,0\,3$ and

$a_2 = 0\,0\,2\,1\,0\,3\,2\,3$

collude and they generate a new codeword *c* = (0 2 2 1 0 2 0 3).

Then $d(a_1, c) = 2$, $d(a_2, c) = 3$, $d(a_3, c) = 6$, $d(a_4, c) = 7$

(ii) if $a_1 = 0\,2\,0\,1\,3\,2\,0\,3$ and

$a_3 = 0\,0\,0\,1\,1\,1\,1\,1$

collude and they generate a new codeword *c* = (0 2 0 1 3 1 1 1).

Then $d(a_1, c) = 2,\ d(a_2, c) = 6,\ d(a_3, c) = 3,\ d(a_4, c) = 5$

(iii) if $a_1 = 0\,2\,0\,1\,3\,2\,0\,3$ and

$a_4 = 0\,0\,2\,1\,0\,3\,2\,3$

collude and they generate a new codeword *c* = (0 2 2 1 0 2 2 3).

Then $d(a_1, c) = 3,\ d(a_2, c) = 4,\ d(a_3, c) = 4,\ d(a_4, c) = 2$

(iv) if $a_2 = 0\,0\,2\,1\,0\,3\,2\,3$ and

$a_3 = 0\,0\,0\,1\,1\,1\,1\,1$

collude and they generate a new codeword *c* = (0 0 0 1 0 1 2 1).

Then $d(a_1, c) = 5,\ d(a_2, c) = 3,\ d(a_3, c) = 2,\ d(a_4, c) = 4$

(v) if $a_2 = 0\,0\,2\,1\,0\,3\,2\,3$ and

$a_4 = 1\,0\,0\,0\,3\,1\,2\,3$

collude and they generate a new codeword *c* = (0 0 2 1 3 3 2 3).

Then $d(a_1, c) = 4,\ d(a_2, c) = 1,\ d(a_3, c) = 4,\ d(a_4, c) = 4$

(vi) if $a_3 = 0\,0\,0\,1\,1\,1\,1\,1$ and

$a_4 = 1\,0\,0\,0\,3\,1\,2\,3$

collude and they generate a new codeword *c* = (0 0 0 1 3 1 2 1).

Then $d(a_1, c) = 4,\ d(a_2, c) = 4,\ d(a_3, c) = 2,\ d(a_4, c) = 3$

It is easy to see that distance *d* is minimum for those codewords a_i and a_j, $1 \le i \le 4, 1 \le j \le 4$ who collude with each other to generate the collusion word c_i. So it is obvious that by the definition of traceable code (TA) given in Fig.1, it is 2-TA code. Now we give the graphical representation of this code C.

Since for each pair of two codewords (a_i, a_j) and any other codeword *x* of code *C* there will be $4C_3$ i.e. 4 cases. Here, each case corresponding to these three codewords is shown pictorially one by one.

Case 1

a_1	0	2	0	1	3	2	0	3
a_2	0	0	2	1	0	3	2	3
a_3	0	0	0	1	1	1	1	1

Case 2

a_1	0	2	0	1	3	2	0	3
a_2	0	0	2	1	0	3	2	3
a_4	1	0	0	0	3	1	2	3

Case 3

a_2	0	0	2	1	0	3	2	3
a_3	0	0	0	1	1	1	1	1
a_4	1	0	0	0	3	1	2	3

Case 4

a_1	0	2	0	1	3	2	0	3
a_3	0	0	0	1	1	1	1	1
a_4	1	0	0	0	3	1	2	3

It is easy to notice that each graph corresponds to the case (ii) of Theorem 3.3, so the above code C again is 2-TA code.

Example 3.3.2: Here we represent an example of a code *C* of distance $d < \frac{2n}{3}$ with $n = 8$ and $d = 4$ and show that this code *C* is not 2-TA code.

$$
\begin{aligned}
c_1 &= 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1\\
c_2 &= 0\ 0\ 0\ 1\ 2\ 2\ 2\ 2\\
c_3 &= 0\ 0\ 1\ 0\ 1\ 1\ 2\ 2\\
c_4 &= 0\ 0\ 1\ 0\ 2\ 2\ 1\ 1\\
c_5 &= 0\ 1\ 0\ 0\ 1\ 2\ 1\ 2\\
c_6 &= 0\ 1\ 0\ 0\ 2\ 1\ 2\ 1\\
c_7 &= 1\ 0\ 0\ 0\ 1\ 2\ 2\ 1\\
c_8 &= 1\ 0\ 0\ 0\ 2\ 1\ 1\ 2
\end{aligned}
$$

If c_1 and c_2 collude and they generate a new codeword c = (0 0 0 1 1 1 2 2), then $d(c_1, c) = 2$, $d(c_2, c) = 2, d(c_3, c) = 2$. In that case an innocent user c_3 will also be traced. So the code C is not a 2-TA code. The pictorial representation of this example is given as

c_1	0	0	0	1	1	1	1	1
c_2	0	0	0	1	2	2	2	2
c_3	0	0	1	0	1	1	2	2

In this case this graph corresponds to the case (i) of Theorem 3.3. So the above code C is not 2-TA code.

4.Conclusion

We have shown pictorially that how an equidistant code of length n with distance d> $\frac{2n}{3}$ is always a 2-TA code and discussed the proofs of theorems for which an equidistant code is not 2-TA code. In future we wish to derive the conditions for an equidistant code to be 3-TA code.

Compliance with ethical standards

Acknowledgments

I am thankful to The Technological Institute of Textile and Sciences, Bhiwani for regular support and motivation.

Disclosure of conflict of interest

There will be no conflict in its publication.

References

[1] Anu Kathuria, Sudhir Batra and S. K. Arora On traceability Property of Equidistant Codes, Discrete Mathematics, Elsevier, vol.340, issue 4, April 2017, pp. 713-721.

[2] Anu Kathuria, Ph.D. Thesis, Combinatorial Properties of some Fingerprinting Models and Linear Codes, Submitted to MDU, Rohtak 2013

[3] N. Wagner, Fingerprinting Techniques, in Proceedings 1983, IEEE Symposium on Security and privacy, pp.18-22, April 1983.

[4] 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.

[5] D. Boneh and J. Shaw ,Collusion Secure fingerprinting for Digital Data, IEEE Transactions on Information Theory, vol. 44, pp. 1897-1905, 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 2007.

[7] B. Chor, A. Fiat and M. Naor, Tracing Traitors, in Advances in Cryptology-CRYPTO 94 (Lecture Notes in Computer Science), vol. 53, no. 2, February 2007.

[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