数理解析研究所講究録
第 1889 巻 2014 年 21-31

Vector Representation of Descendant Sets and Binary Fingerprinting Codes

Ryoh Fuji-Hara
Faculty of Engineering, Information and System, University of Tsukuba, Japan
fujihara@sk.tsukuba.ac.jp

Abstract

Let S be a finite set of q symbols and $C \subseteq S^n$. $C(i)$ is the set of S consisting of the elements appear in the i-th coordinate of C, $C(i) = \{c_i \mid (c_1.c_2, ..., c_n) \in C\}$. The decedent set of C, $desc(C)$, is the set of all possible n-tuples of S^n such that the elements at the i-th coordinate of $desc(C)$ are from $C(i)$.

$$desc(C) = C(1) \times C(2) \times \cdots \times C(n)$$

The n-tuples of C are called *parents*. There are several codes defined by using descendant sets. Here we consider a code called *$t-$separable code.* It is a set of n-tuples $\mathfrak{C} \subset S^n$ satisfying $desc(C) \neq desc(D)$ for any $C, D \subseteq \mathfrak{C}$ such that $C \neq D$ and $|C|, |D| \leq t$. In the case $|S| = 2$ and $t = 2$, we discuss a way to represent descendant sets, basic properties of descendant sets and constructions of t-separable codes, etc.

1 Introduction

Let S be a finite set of q symbols and $C \subset S^n$. $C(i)$ is the set of S consisting of the elements appear in the i-th coordinate of C.

$$C(i) = \{c_i \mid (c_1.c_2, ..., c_n) \in C\}$$

The decedent set of C denoted by $desc(C)$ is the set of all possible n-tuples of S^n such that the elements at the i-th coordinate of $desc(C)$ are from $C(i)$.

$$desc(C) = C(1) \times C(2) \times \cdots \times C(n)$$

The n-tuples of C are called *parents.*

Example 1.1 *Let* $S = \{0,1\}, C = \{(1,0,1,0), (1,1,0,0)\}$, *then* $desc(C) = \{1\} \times \{0,1\} \times \{0,1\} \times \{0\} = \{(1,0,0,0), (1,0,1,0), (1,1,0,0), (1,1,1,0)\}$.

There are several codes defined by descendant sets which are used in digital fingerprinting. t-Frameproof code and t-secure frameproof code were defined by D. Boneh and J. Shaw (1998) [2], t-identifying parent property code by H. D. L. Hollmann, J. H. van Lint, J-P. Linnartz and L. M. G. M. Tolhuizen (1998) [12], t-traceability code by B. Chor, A. Fiat and M. Noor [7], t-expanded separable code by M. Cheng et. al., etc. We call these generally *fingerprinting codes.* The underlying problems of the fingerprinting code can be seen in [2] , [8], [11], [16] . Combinatorial approaches to analysis and construction of fingerprinting codes are seen in [1], [15].

Here we consider a code called $t-$*separable code* . It is a set of n-tuples $\mathfrak{C} \subset S^n$ satisfying $desc(C) \neq desc(D)$ for any $C, D \subset \mathfrak{C}$ such that $C \neq D$ and $|C|, |D| \leq t$. We denote it $t - SC(n, M, |S|)$, where $M = |\mathfrak{C}|$ is the number of code words.

The code is defined by M. Cheng and Y. Miao (2012) [5], and it is the most basic code because every other codes mentioned above have to satisfy the condition of t-separable code[13], which means these fingerprinting codes are all subsets of t-separable codes.

M. Cheng and Y. Miao [5] have shown an upper bound on the size of 2-separable codes: If there exists a $2 - SC(n, M, q)$ then

$$M \leq q^{n-1} + q(q-1)/2.$$

Note that F. Gao and G. Ge [10] recently made better bound:

$$M \leq \frac{3}{2} q^{2\lceil \frac{n}{3} \rceil} - \frac{1}{2} q^{\lceil \frac{n}{3} \rceil}.$$

We disscuss here the simplest case of t-separable codes, that is, the case of $|S| = 2$ and $t = 2$.

2 Descendant Vector

Constructions of the codes defined by descendant sets are very difficult problems. The main reason of the difficulty is caused by a set theoretical definition of descendant sets. Here we represent a descendant set by a vector over an algebra.

Let $S = \{0, 1\}$. The set of n-tuples of S deals with the set of n-dimensional vectors over the finite field of order 2, ${F_2}^n$.

Definition 2.1 *For any* $\mathbf{x}, \mathbf{y} \in {F_2}^n$,

$$dv(\mathbf{x}, \mathbf{y}) := \mathbf{x} * \mathbf{y} + alf(\mathbf{x} + \mathbf{y}),$$

where $*, +$ *are multiplication and addition over* F_2*, respectively.* $alf(0) = 0, alf(1) = \alpha$ *and* α *is an indeterminate. Apply the operations for each coordinate of* ${F_2}^n$.

Example 2.2 $\mathbf{x} = (1,0,1,0), \mathbf{y} = (1,1,0,0)$,

$$desc(\mathbf{x},\mathbf{y}) = \{1\} \times \{0,1\} \times \{0,1\} \times \{0\},$$

$$dv(\mathbf{x},\mathbf{y}) = (1,\alpha,\alpha,0)$$

If the set of symbols of S which appears in the i-th coordinate $C(i)$ is $\{0,1\}$, then the i-th position of descendant vector turns out α. For the descendant vector of parents $C \subseteq {F_2}^n$ such that $|C| \geq 3$, we need to define an algebra over the set $\mathcal{A} = \{0,1,\alpha,\alpha+1\}$.

Definition 2.3

$$1 * \alpha = \alpha * 1 = 1 \textit{ and } \alpha * \alpha = \alpha$$

From the definition, we have the following multiplication table:

$*$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	1	0
α	0	1	α	$\alpha+1$
$\alpha+1$	0	0	$\alpha+1$	$\alpha+1$

The addition on $\mathcal{A}$ is naturally computed as polynomials over F_2. In deed, the algebra with the multiplication and addition on $\mathcal{A}$ is isomorphic to the ring $F_2 \times F_2$ with the correspondence $0 = (0,0), 1 = (0,1), \alpha = (1,1), \alpha+1 = (1,0)$.

Now we define the descendant vector for parents of general size.

Definition 2.4 *Suppose $dv(C)$ is defined for a subset C of ${F_2}^n$. Let $\mathbf{x} \in {F_2}^n \setminus C$,*

$$dv(C \cup \{\mathbf{x}\}) := dv(C) * \mathbf{x} + alf(dv(C) + \mathbf{x}),$$

where

$$alf(z) = \begin{cases} \alpha & \text{if } z = 1 \\ z & \text{otherwise} \end{cases}$$

for any $z \in A$

Lemma 2.5 *For any $d \in \{0,1,\alpha\}$ and $x \in \{0,1\}$, $d * x + alf(d+x) \in \{0,1,\alpha\}$.*

Proof When $d = 0$ or 1, it is obvious. We consider the case $d = \alpha$ and $x \in \{0,1\}$. If $d = \alpha$ and $x = 0$, then $\alpha * 0 + alf(\alpha + 0) = 0 + \alpha = \alpha$. If $d = \alpha$ and $x = 1$, then $\alpha * 1 + alf(\alpha+1) = 1 + (\alpha+1) = \alpha$ □

From this lemma, descendant vector does not contain $\alpha+1$, that is $dv(C) \in \{0,1,\alpha\}^n$ for any $C \subseteq F_2{}^n$.

Lemma 2.6

$$dv(\{\mathbf{x},\mathbf{y}\} \cup \{\mathbf{z}\}) = dv(\{\mathbf{x},\mathbf{z}\} \cup \{\mathbf{y}\})$$

Consider possible combinations of i-th coordinate of $\mathbf{x},\mathbf{y},\mathbf{z}$. The possible combinations of $0, 1$ are only 8. It is not difficult check all 8 cases. The lemma implies the definition of descendant vector is well-defined.

Example 2.7

$$\begin{array}{lcllll} dv(\mathbf{x},\mathbf{y}) & = & (1, & \alpha, & \alpha, & 0) \\ \mathbf{z} & = & (0, & 1, & 0, & 0) \\ dv(\mathbf{x},\mathbf{y}) * \mathbf{z} & = & (0, & 1, & 0, & 0) \\ alf(dv(\mathbf{x},\mathbf{y}) + \mathbf{z}) & = & (\alpha, & \alpha+1, & \alpha, & 0) \\ dv(\mathbf{x},\mathbf{y},\mathbf{z}) & = & (\alpha, & \alpha, & \alpha, & 0) \end{array}$$

$C(i)$ is the set of symbols which appear in i-th coordinate of each $\mathbf{x} \in C$, for any $C \subset F_2{}^n$. $C(i)$ is $\{0\}, \{1\}$, or $\{0,1\}$. Each coordinate of a descendant vector has an element $0, 1$ or α which corresponds to $\{0\}, \{1\}$, or $\{0,1\}$ of $C(i)$, respectively. Therefore, we have the following theorem:

Theorem 2.8 *For any subsets $C, D \subseteq F_2{}^n$, $desc(C) = desc(D)$ if and only if $dv(C) = dv(D)$.*

3 Basic Properties

The theorem 2.8 means that any descendant set is represented by a vector on the algebra A. Therefore, the set theoretical operations on descendant sets can be replaced by algebraic operations on A. We see basic properties of the correspondences. Those may be useful for constructions of fingerprinting codes.

Lemma 3.1 *For any $C, D \subseteq F_2{}^n$, $desc(C) \cap desc(D) = \phi$ if and only if there exists an element 1 of S as a coodinate in the vector $dv(C) + dv(D)$.*

The proof is seen in [9].

Example 3.2

$$\begin{array}{lclllll} dv(C) & = & (1, & 0, & \alpha, & \alpha, & \alpha, & 0) \\ dv(D) & = & (1, & 0, & 1, & 0, & \alpha, & 1) \\ dv(C)+dv(D) & = & (0, & 0, & \alpha+1, & \alpha, & 0, & 1) \end{array}$$

Lemma 3.3 *For any* $\mathbf{x} \in F_2{}^n$ *and* $C \subset F_2{}^n$, *the followings are equivalent:*

1. $\mathbf{x} \in desc(C)$,
2. *there exists no element* 1 *in* $dv(C) + \mathbf{x}$,
3. $dv(C) = dv(C \cup \{\mathbf{x}\})$.

The proof is seen in [9].

Lemma 3.4 *For any* $\mathbf{x} \in F_2{}^n$ *and* $C \subset F_2{}^n$, *if* $\mathbf{x} \in desc(C)$ *then* $dv(C) * \mathbf{x} = \mathbf{x}$.

The proof is seen in [9]. I

Lemma 3.5 *For any* $C, D \subset F_2{}^n$, $C \neq D$, $desc(C) \subset desc(D)$ *if and only if the following conditions are satisfied:*

- $dv(C) * dv(D) = dv(C)$ *and*
- $dv(C) + dv(D)$ *contains no element* 1.

The proof is seen in [9].

Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ be a (0,1)-vector. The function $supp(\mathbf{x})$ is offen used as the following definition:

$$supp(\mathbf{x}) = \{i \mid x_i = 1, 1 \leq i \leq n\}.$$

Then, $\mathbf{x} * \mathbf{y} = \mathbf{x}$ implies $supp(\mathbf{x}) \subseteq supp(\mathbf{y})$. Here we denote the relation $\mathbf{x} \preceq \mathbf{y}$ if $\mathbf{x} * \mathbf{y} = \mathbf{x}$ for any $\mathbf{x}, \mathbf{y} \in \mathcal{A}^n$

Lemma 3.6 *For any* $C, D \subset F_2{}^n$, *when* $C \cap D \neq \phi$, *then the following holds:*

$$dv(C \cap D) \preceq dv(C) * dv(D).$$

The proof is seen in [9]. **Proof**

Example 3.7

$$\begin{array}{lcl} C & = & \{(1,0,1,0,0),(1,0,0,1,0)\} \\ D & = & \{(1,0,1,0,0),(1,0,1,1,1)\} \\ dv(C) & = & (1,0,\alpha,\alpha,0) \\ dv(D) & = & (1,0,1,\alpha,\alpha) \\ dv(C) * dv(D) & = & (1,0,1,\alpha,0) \\ dv(C \cap D) & = & (1,0,1,0,0) \end{array}$$

Lemma 3.8 *Let* $C \subseteq F_2{}^n$ *and* $\mathbf{x},, \mathbf{y} \in F_2{}^n$.

$$\begin{array}{rcl} dv(C \cup \{\mathbf{x}, \mathbf{y}\}) & = & dv(C) * dv(\mathbf{x}, \mathbf{y}) + alf(dv(C) + dv(\mathbf{x}.\mathbf{y})) \\ & = & dv(C \cup \{x\}) * dv(\mathbf{y}) + alf(dv(C \cup \{\mathbf{x}\}) + dv(\mathbf{y})) \end{array}$$

The proof of the lemma can be done by verifying all possible case. Let x_i and y_i be i-th coordinates of $\mathbf{x}$ and $\mathbf{y}$, respectively. The all possible elements are $C(i) = \{0\}, \{1\}$ or $\{0,1\}$ and $x_i = 0$ or 1 , $y_i = 0$ or 1. Totally only 12 cases.

Lemma 3.9 *For any $C, D \subset {F_2}^n$,*

$$dv(C \cup D) = dv(C) * dv(D) + alf(dv(C) + dv(D))$$

The proof is seen in [9].

4 Geometrical Constructions of 2-separable codes

Consider that each vector of ${F_2}^n$ except the zero vector is a point of finite projective geometry PG$(n-1,2)$. Then for any distinct points $\mathbf{x}, \mathbf{y} \in {F_2}^n \setminus \{0\}$, the set of three points $\{\mathbf{x}, \mathbf{y}, \mathbf{x+y}\}$ is a line of PG$(n-1,2)$.

Lemma 4.1 *For any four distinct points of PG$(n-1,2)$, $C_0 = \{\mathbf{x}_0, \mathbf{y}_0\}, C_1 = \{\mathbf{x}_1, \mathbf{y}_1\}$, $dv(C_0) = dv(C_1)$ if and only if $\mathbf{x}_0 * \mathbf{y}_0 = \mathbf{x}_1 * \mathbf{y}_1$ and $\mathbf{x}_0 + \mathbf{y}_0 = \mathbf{x}_1 + \mathbf{x}_1$.*

The proof is seen in [9].

Theorem 4.2 *For any four points $\mathbf{x}_0, \mathbf{y}_0, \mathbf{x}_1, \mathbf{y}_1$ of PG$(n-1,2)$ such that $\{\mathbf{x}_0, \mathbf{y}_0\} \neq \{\mathbf{x}_1, \mathbf{y}_1\}$, $dv(\mathbf{x}_0, \mathbf{y}_0) = dv(\mathbf{x}_1, \mathbf{y}_1)$ if and only if the followings are satisfied:*

(i) $\mathbf{x}_0 + \mathbf{y}_0 = \mathbf{x}_1 + \mathbf{y}_1 = \mathbf{h}$ (*which implies* $\mathbf{x}_0 + \mathbf{x}_1 = \mathbf{y}_0 + \mathbf{y}_1 = \mathbf{d}$) *and*

(ii) $\mathbf{d} * \mathbf{h} = \mathbf{d}$ (*i.e.* $\mathbf{d} \preceq \mathbf{h}$)

Proof If $\mathbf{x}_0 + \mathbf{y}_0 \neq \mathbf{x}_1 + \mathbf{y}_1$, clearly $dv(\mathbf{x}_0, \mathbf{y}_0) \neq dv(\mathbf{x}_1, \mathbf{y}_1)$. Therefore, we consider the case $\mathbf{x}_0 + \mathbf{y}_0 = \mathbf{x}_1 + \mathbf{y}_1$. Then, from Lemma 4.1,

$$\mathbf{x}_0 * \mathbf{y}_0 = \mathbf{x}_1 * \mathbf{y}_1 \text{ if and only if } dv(\mathbf{x}_0, \mathbf{y}_0) = dv(\mathbf{x}_1, \mathbf{y}_1)$$

Since $\mathbf{x}_1 = \mathbf{x}_0 + \mathbf{d}$ and $\mathbf{y}_1 = \mathbf{y}_0 + \mathbf{d}$,

$$\begin{aligned} \mathbf{x}_1 * \mathbf{y}_1 &= (\mathbf{x}_0 + \mathbf{d}) * (\mathbf{y}_0 + \mathbf{d}) \\ &= \mathbf{x}_0 * \mathbf{y}_0 + \mathbf{x}_0 * \mathbf{d} + \mathbf{y}_0 * \mathbf{d} + \mathbf{d} \\ &= \mathbf{x}_0 * \mathbf{y}_0 + \mathbf{d} * (\mathbf{x}_0 + \mathbf{y}_0 + \mathbf{d}'), \end{aligned}$$

where $\mathbf{d}'$ is a vector such that $\mathbf{d} * \mathbf{d}' = \mathbf{d}$. From the equation, $\mathbf{x}_1 * \mathbf{y}_1 = \mathbf{x}_0 * \mathbf{y}_0$ if and only if $\mathbf{d} * (\mathbf{x}_0 + \mathbf{y}_0 + \mathbf{d}') = 0$.

The necessary and sufficient condition for $\mathbf{d} * (\mathbf{x}_0 + \mathbf{y}_0 + \mathbf{d}') = 0$ is $\mathbf{x}_0 + \mathbf{y}_0 = \mathbf{d}'$ or $\mathbf{d} * (\mathbf{x}_0 + \mathbf{y}_0) = \mathbf{d} * \mathbf{h} = \mathbf{d}$ (including the case $\mathbf{d} = \mathbf{x}_0 + \mathbf{y}_0$).

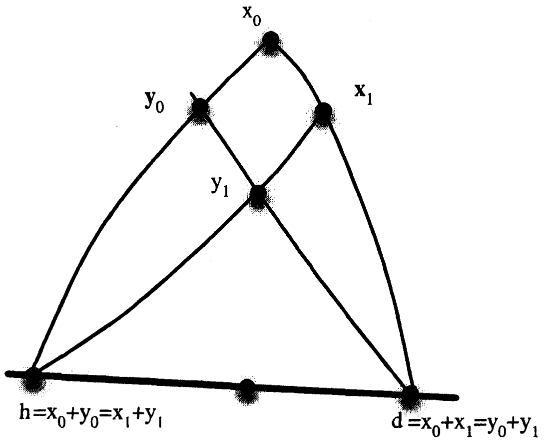

Figure 1:

In the case $\mathbf{d} = \mathbf{x}_0 + \mathbf{y}_0$:

$$\mathbf{x}_1 = \mathbf{x}_0 + \mathbf{d} = \mathbf{x}_0 + \mathbf{x}_0 + \mathbf{y}_0 = \mathbf{y}_0$$

$$\mathbf{y}_1 = \mathbf{y}_0 + \mathbf{d} = \mathbf{y}_0 + \mathbf{x}_0 + \mathbf{y}_0 = \mathbf{x}_0$$

This contradicts $\{\mathbf{x}_0, \mathbf{y}_0\} \neq \{\mathbf{x}_1, \mathbf{y}_1\}$.
In the case $\mathbf{x}_0 + \mathbf{y}_0 = \mathbf{d}'$:

$$\mathbf{d} * (\mathbf{x}_0 + \mathbf{y}_0) = \mathbf{d} * \mathbf{d}' = \mathbf{d}.$$

Therefore, (i) and (ii) are the necessary and sufficient conditions for $dv(\mathbf{x}_0, \mathbf{y}_0) = dv(\mathbf{x}_1, \mathbf{y}_1)$ □

A set of four points on a plane, no three of which are collinear, is called a *quadrangle.* Let Q ba a quadrangle in a plane of order 2. Then there is exactly one line in the plane which is not incident with any point of Q. The line is called a *external line* to Q. Theorem 4.2 says that if $Q = \{\mathbf{x}_0, \mathbf{y}_0, \mathbf{x}_1, \mathbf{y}_1\}$ is a quadrangle and the external line to Q contains two points $\mathbf{d}, \mathbf{h}$ such that $\mathbf{d} \preceq \mathbf{h}$, then the four points Q can not be contained in a 2-SC(n,M,2).

The lines in PG(n-1,2) contains two points $\mathbf{d}, \mathbf{h}$ such that $\mathbf{d} \preceq \mathbf{h}$ play an important role for construction of 2-SC(n,M,2). We call here such a line an *i-line.* When a line containing the points $\mathbf{d}, \mathbf{h}$ is an *i*-line (i.e. $\mathbf{d} \preceq \mathbf{h}$), the third point $\mathbf{p} = \mathbf{d} + \mathbf{h}$ on the line and $\mathbf{d}$ has the relation $\mathbf{p} * \mathbf{d} = \mathbf{0}$, which means $supp(\mathbf{p}) \cap supp(\mathbf{d}) = \phi$.

Lemma 4.3 *Let* $\mathfrak{C} \subset F_2{}^n$ *be a 2-SC(n,M,2) not including the zero vector* $\mathbf{0}$. $\mathfrak{C} \cup \{\mathbf{0}\}$ *is a 2-SC(n,M+1,2) if and only if* $\mathfrak{C}$ *contains no three points on any i-line.*

The proof is seen in [9].

In the case of $n = 3$, the vectors of ${F_2}^3$ except $\mathbf{0}$ correspond to the points of PG(2,2) called Fano plane. In the Fano plane, the line $l = \{(0,1,1),(1,1,0),(1,0,1)\}$ is only the non i-line. All the others are i-lines. $D = \{((1,0,0),(0,1,0),(0,0,1),(1,1,1)\}$ is the unique quadrangle not meet the line l. Therefore, $D \cup \{\mathbf{0}\}$ or $D \cup \mathbf{p}$, where $\mathbf{p}$ is a point on the line l, are 2-SC(3,5,2), which contain the maximal number of code words.

Consider PG(n-1,2) , $n \geq 4$. From Theorem 4.2, we have the following theorem:

Theorem 4.4 *Let $\mathfrak{C}$ be a set of points in PG(n-1,2). $\mathfrak{C}$ is a 2-separable code if and only if , for each plane $\mathcal{P}$ in PG(n-1,2), the points of $\mathfrak{C} \cap \mathcal{P}$ contains*

- *no quadrangle or*
- *a quadrangle Q but the external line to Q is a non i-line.*

Corollary 4.5 *Let l, m be lines of PG(3,2) which are not concurrent. Then the 6 points, $\mathfrak{C}$, on the lines are 2-SC(4,6,2). If those two lines are non i-lines then $\mathfrak{C} \cup \{\mathbf{0}\}$ is 2-SC(4,7,2).*

Let $\mathcal{F}$ be a set of points in PG(n-1,2). For any two points of $\mathcal{F}$, if the line passing through the two points is contained in $\mathcal{F}$, then $\mathcal{F}$ is called a *flat.* A d-flat is a flat generated from $d+1$ independent vectors. If a d-flat contains no i-line, then it is said to be *i-line free d-flat.*

Theorem 4.6 *Let $\mathcal{F}$ be an i-line free d-flat of PG(n-1,2), and $\mathcal{W}$ be a (d+1)-flat including $\mathcal{F}$. Then the the set of points of $\mathcal{A} = \mathcal{W} \setminus \mathcal{F}$ is a $2-SC(n, 2^{d+1}, 2)$. Further, $\mathcal{A} \cup \{\mathbf{0}\}$ is a $2-SC(n, 2^{d+1}+1, 2)$.*

The proof is seen in [9].

5 i-line free flats

Theorem 4.6 says if there is a large i-line free d-flat, there exists a 2-separable code with a large number of code words. So it is important to find an i-line free d-flat, and d as large as possible.

In order to find an i-line free d-flats, let's count the number of i-lines.

Lemma 5.1 *Le P be a point of PG(n-1,2). The number of i-lines incident with P is*

$$2^{n-w} + 2^{w-1} - 2,$$

where w is Hamming weight of P.

The proof is seen in [9].

Lemma 5.2 *The number of i-lines in PG(n-1,2) is*

$$\frac{1}{3}\sum_{w=1}^{n}\binom{n}{w}(2^{n-w}+2^{w-1}-2)$$

$$= (3^n - 2^{n+1} + 1)/2.$$

The proof is seen in [9].

The number of lines in PG(n-1,2) is $(2^n-1)(2^{n-1}-1)/3$. The ratio of i-lines to the all lines in PG(n-1,2) is

$$\frac{3^{n+1}-3(2^{n+1})+3}{(2^n-2)\,(2^n-1)}$$

This reduces exponentially. The ratios are, for examples, 0.85 when n=3, 0.58 when n=5, 0.16 when n=10 and 0.0095 when n=20. The trend of ratios suggests there may exist large i-line free flat. We are interested in how large the flats in PG(n-1,2) are.

Here is the i-line free 1-flat in PG(2,2) which is the largest:

$$(1,1,0),(1,0,1),(0,1,1)$$

An i-line free 2-flat is the following, which appears in PG(5,2).

$$\begin{array}{c}(1,1,0,0,1,1)\\(0,0,1,1,1,1)\\(1,1,1,1,0,0)\\(1,0,0,1,1,0)\\(0,1,1,0,1,0)\\(1,0,1,0,0,1)\\(0,1,0,1,0,1)\end{array}$$

From my experiments, there is no i-line free plane in PG(3,2), PG(4,2).

If there exist an i-line free hyperplane in PG(n-1,2), then we can have a 2-SC$(n,2^{n-1}+1,2)$ which attains the Cheng-Miao Bound. Unfortunately, we have the following result:

Lemma 5.3 (A. Munemasa [14]) *There is no i-line free hyperplane of PG*$(n-1,\ 2)$ *for* $n \geq 4$.

The proof is seen in [9].

Lemma 5.4 *Let* $\mathcal{F}$ *be a linear subspace in* ${F_2}^n$ *excluding* $\mathbf{0}$. *If, for any two vectors* $\mathbf{x},\mathbf{y}\in\mathcal{F}$, $|supp(\mathbf{x})\cap supp(\mathbf{y})|\geq 1$, *then* $\mathcal{F}$ *is i-line free.*

The proof is seen in [9].

Let V be a finite set with v element and $\mathcal{B}$ a collection of k-subsets of V. If $v = 4d - 1, k = 2d$ and $|B \cap B'| = d$ for any $B, B' \in \mathcal{B}$, then the pair $(V, \mathcal{B})$ is called an *Hadamard design.*

Lemma 5.5 *The incidence matrix of an Hadamard design which is linear on ${F_2}^n$ is an i-line flat.*

A simplex code is the dual code of the Hamming code of length $2^m - 1, m \geq 2$. It is well known that a simplex code excluding **0** is an Hadamard design with the parameters $v = 2^m - 1, k = 2^{m-1}, d = 2^{m-2}$ and it is a d-flat in the PG$(2^m - 2, 2)$.

Example 5.6 *An simplex code (i-line free 2-flat in PG(6,2))*

$$\begin{array}{c} (0,1,1,0,0,1,1) \\ (0,0,0,1,1,1,1) \\ (0,1,1,1,1,0,0) \\ (1,1,0,0,1,1,0) \\ (1,0,1,1,0,1,0) \\ (1,1,0,1,0,0,1) \\ (1,0,1,0,1,0,1) \end{array}$$

Theorem 5.7 *There exists i-line free (2^{m-2})-flat in PG$(2^m - 2, 2)$ for any integer $m \geq 2$.*

Let H be an incidence matrix of a Hadamard design with the parameters $v = 2^m - 1, k = 2^{m-1}, d = 2^{m-2}$. An array H' obtained by punctuating at most $d - 1$ coordinates of H is also i-line free flat.

Conjecture 5.8 (A. Munemasa [14]) *If $\mathcal{F}$ is an i-line free flat, then $\mathcal{F}$ is obtained from either of*

(1) *an simplex code or its subspace,*

(2) *punctuating some coordinates from (1).*

References

[1] S. R. Blackburn, Combinatorial schemes for protecting digital content, In: Surveys in Combinatorics 2003, Cambridge Univ. Press, 2003, pp. 43–78.

[2] D. Boneh and J. Shaw, Collusion-secure fingerprinting for digital data, IEEE Trans. Inform. Theory 44 (1998), 1897–1905.

[3] M. Cheng, H.Fu, J. Jiang, Y. Lo and Y. Miao, New Bound on $\bar{2}$-separable codes of length 2, Designs, Codes and Cryptography, to appear

[4] M.Cheng, H. Fu, J. Jiang, Y. Lo and Y. Miao, Expanded Separable Code, submitted

[5] M. Cheng, L. Ji and Y. Miao, Separable codes, IEEE Trans. Inform. Theory, 58 (2012), 1791–1803.

[6] M. Cheng and Y. Miao, On anti-collusion codes and detection algorithms for multimedia fingerprinting, IEEE Trans. Inform. Theory, 57 (2011), 4843–4851.

[7] B. Chor, A. Fiat, M. Naor and B. Pinkas, Tracing traitors, IEEE Trans. Inform. Theory 46 (2000), 893–910.

[8] B. Chor, A. Fiat and M Naor, Tracing traitors, in Crypto '94, LCS 839, 1994, 257-270

[9] R. Fuji-Hara, Descendant Sets and Code of Binary Case, submitted

[10] F. Gao and G. Ge, New Bounds on separable codes, submitted

[11] K. J. R. Liu, W. Trappe, Z. J. Wang, M. Wu, and H. Zhao, Multimedia Fingerprinting Forensics for Traitor Tracing, Hindawi, 2005.

[12] H. D. L. Hollmann, J. H. van Lint, J-P. Linnartz and L. M. G. M. Tolhuizen, On codes with the identifiable parent property, J. Combin. Theory Ser. A 82 (1998), 121–133.

[13] Y. Miao, Faculty of Engineering, Information and System, University of Tsukuba, Personal Communication (2013)

[14] A. Munemasa, Graduate School of Information Sciences, Tohoku University, Personal communication (2012)

[15] D. R. Stinson, T. van Trung and R. Wei, Secureframe proof codes, key distribution patterns, group testing algorithms and related structures, J. Statist. Plann. Inference 86 (2000), 595–617.

[16] M. Wu, W. Trappe, Z. J. Wang and K. J. R. Liu, Collusion- resistant fingerprinting for multimedia, IEEE Signal Processing Magazine 21 (2004), 15–27.