<table>
<thead>
<tr>
<th>Title</th>
<th>Vector Representation of Descendant Sets and Binary Fingerprinting Codes (Designs, Codes, Graphs and Related Areas)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Fuji-Hara, Ryoh</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 (2014), 1889: 21-31</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2014-04</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/195758">http://hdl.handle.net/2433/195758</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>

Kyoto University
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 $C$, $C(i) = \{c_i \mid (c_1, c_2, \ldots, c_n) \in C\}$. The decedent set of $C$, $\text{desc}(C)$, is the set of all possible $n$-tuples of $S^n$ such that the elements at the $i$-th coordinate of $\text{desc}(C)$ are from $C(i)$.

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

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 $\mathcal{C} \subset S^n$ satisfying $\text{desc}(C) \neq \text{desc}(D)$ for any $C, D \subseteq \mathcal{C}$ 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 $C$.

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

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

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

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 $\text{desc}(C) = \{1\} \times \{0, 1\} \times \{0, 1\} \times \{0\} = \{(1, 0, 0, 0), (1, 0, 1, 0), (1, 1, 0, 0), (1, 1, 1, 0)\}$.
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. 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 $\mathcal{C} \subset S^n$ satisfying $\text{desc}(C) \neq \text{desc}(D)$ for any $C, D \subset \mathcal{C}$ such that $C \neq D$ and $|C|, |D| \leq t$. We denote it $t - SC(n, M, |S|)$, where $M = |\mathcal{C}|$ 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 discuss 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 $x, y \in F_2^n$,

$$dv(x, y) := x \ast y + alf(x + y),$$

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


Example 2.2 \( x = (1, 0, 1, 0), y = (1, 1, 0, 0), \)
\[
\text{desc}(x, y) = \{1\} \times \{0, 1\} \times \{0, 1\} \times \{0\},
\]
\[
dv(x, y) = (1, \alpha, \alpha, 0)
\]

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 \( \alpha \). 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

\[ 1 \ast \alpha = \alpha \ast 1 = 1 \quad \text{and} \quad \alpha \ast \alpha = \alpha \]

From the definition, we have the following multiplication table:

\[
\begin{array}{c|cccc}
* & 0 & 1 & \alpha & \alpha + 1 \\
\hline
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 \\
\alpha & 0 & 1 & \alpha & \alpha + 1 \\
\alpha + 1 & 0 & 0 & \alpha + 1 & \alpha + 1 \\
\end{array}
\]

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 \( x \in F_2^n \setminus C \),
\[ dv(C \cup \{x\}) := dv(C) \ast x + alf(dv(C) + x), \]
where
\[ alf(z) = \begin{cases} 
\alpha & \text{if } z = 1 \\
\text{otherwise} & \end{cases} 
\]
for any \( z \in \mathcal{A} \)

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

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 \( \alpha \ast 0 + alf(\alpha + 0) = 0 + \alpha = \alpha \). If \( d = \alpha \) and \( x = 1 \), then \( \alpha \ast 1 + alf(\alpha + 1) = 1 + (\alpha + 1) = \alpha \) \( \square \)
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**

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

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

**Example 2.7**

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

$$z = (0, 1, 0, 0)$$

$$dv(x, y) * z = (0, 1, 0, 0)$$

$$al i f (dv(x, y) + z) = (\alpha, \alpha + 1, \alpha, 0)$$

$$dv(x, y, z) = (\alpha, \alpha, \alpha, 0)$$

$C(i)$ is the set of symbols which appear in $i$-th coordinate of each $x \in C$, 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 $\alpha$ 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**

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 coordinate in the vector $dv(C) + dv(D)$.

The proof is seen in [9].

**Example 3.2**

$$dv(C) = (1, 0, \alpha, \alpha, \alpha, 0)$$

$$dv(D) = (1, 0, 1, 0, \alpha, 1)$$

$$dv(C) + dv(D) = (0, 0, \alpha + 1, \alpha, 0, 1)$$
Lemma 3.3 For any $x \in F_2^n$ and $C \subset F_2^n$, the followings are equivalent:

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

The proof is seen in [9].

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

The proof is seen in [9].

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

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

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

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

<table>
<thead>
<tr>
<th>$C$</th>
<th>${(1,0,1,0,0), (1,0,0,1,0)}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D$</td>
<td>${(1,0,1,0,0), (1,0,1,1,1)}$</td>
</tr>
<tr>
<td>$dv(C)$</td>
<td>$(1,0,\alpha,\alpha,0)$</td>
</tr>
<tr>
<td>$dv(D)$</td>
<td>$(1,0,1,\alpha,\alpha)$</td>
</tr>
<tr>
<td>$dv(C) * dv(D)$</td>
<td>$(1,0,1,\alpha,0)$</td>
</tr>
<tr>
<td>$dv(C \cap D)$</td>
<td>$(1,0,1,0,0)$</td>
</tr>
</tbody>
</table>

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

$$dv(C \cup \{x, y\}) = dv(C) * dv(x, y) + alf(dv(C) + dv(x, y))$$
$$= dv(C \cup \{x\}) * dv(y) + alf(dv(C \cup \{x\}) + dv(y))$$
The proof of the lemma can be done by verifying all possible case. Let $x_i$ and $y_i$ be $i$-th coordinates of $x$ and $y$, 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 $C,D \subset F_2^n$,

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

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 $x,y \in F_2^n \setminus \{0\}$, the set of three points $\{x, y, x+y\}$ is a line of $PG(n-1,2)$.

**Lemma 4.1** For any four distinct points of $PG(n-1,2)$, $C_0 = \{x_0, y_0\}, C_1 = \{x_1, y_1\}$, $dv(C_0) = dv(C_1)$ if and only if $x_0 \ast y_0 = x_1 \ast y_1$ and $x_0 + y_0 = x_1 + x_1$.

The proof is seen in [9].

**Theorem 4.2** For any four points $x_0, y_0, x_1, y_1$ of $PG(n-1,2)$ such that $\{x_0, y_0\} \neq \{x_1, y_1\}$, $dv(x_0, y_0) = dv(x_1, y_1)$ if and only if the followings are satisfied:

(i) $x_0 + y_0 = x_1 + y_1 = h$ (which implies $x_0 + x_1 = y_0 + y_1 = d$) and

(ii) $d \ast h = d$ (i.e. $d \preceq h$)

**Proof** If $x_0 + y_0 \neq x_1 + y_1$, clearly $dv(x_0, y_0) \neq dv(x_1, y_1)$. Therefore, we consider the case $x_0 + y_0 = x_1 + y_1$. Then, from Lemma 4.1,

$$x_0 \ast y_0 = x_1 \ast y_1$$

if and only if $dv(x_0, y_0) = dv(x_1, y_1)$

Since $x_1 = x_0 + d$ and $y_1 = y_0 + d$,

$$x_1 \ast y_1 = (x_0 + d) \ast (y_0 + d)$$

$$= x_0 \ast y_0 + x_0 \ast d + y_0 \ast d + d$$

$$= x_0 \ast y_0 + d \ast (x_0 + y_0 + d'),$$

where $d'$ is a vector such that $d \ast d' = d$. From the equation, $x_1 \ast y_1 = x_0 \ast y_0$ if and only if $d \ast (x_0 + y_0 + d') = 0$.

The necessary and sufficient condition for $d \ast (x_0 + y_0 + d') = 0$ is $x_0 + y_0 = d'$ or $d \ast (x_0 + y_0) = d \ast h = d$ (including the case $d = x_0 + y_0$).
In the case $d = x_0 + y_0$:

$$x_1 = x_0 + d = x_0 + x_0 + y_0 = y_0$$
$$y_1 = y_0 + d = y_0 + x_0 + y_0 = x_0$$

This contradicts $\{x_0, y_0\} \neq \{x_1, y_1\}$.

In the case $x_0 + y_0 = d'$:

$$d * (x_0 + y_0) = d * d' = d.$$

Therefore, (i) and (ii) are the necessary and sufficient conditions for $dv(x_0, y_0) = dv(x_1, y_1)$.

A set of four points on a plane, no three of which are collinear, is called a quadrangle.

Let $Q$ be 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 $Q = \{x_0, y_0, x_1, y_1\}$ is a quadrangle and the external line to $Q$ contains two points $d, h$ such that $d \preceq h$, 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 $d, h$ such that $d \preceq h$ 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 $d, h$ is an i-line (i.e. $d \preceq h$), the third point $p = d + h$ on the line and $d$ has the relation $p * d = 0$, which means $supp(p) \cap supp(d) = \phi$.

**Lemma 4.3** Let $\mathcal{C} \subset F_2^n$ be a 2-SC(n,M,2) not including the zero vector $0$. $\mathcal{C} \cup \{0\}$ is a 2-SC(n,M+1,2) if and only if $\mathcal{C}$ 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 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, \( D \cup \{0\} \) or \( D \cup p \), where \( p \) 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 \( \mathcal{C} \) be a set of points in \( PG(n-1,2) \). \( \mathcal{C} \) is a 2-separable code if and only if, for each plane \( \mathcal{P} \) in \( PG(n-1,2) \), the points of \( \mathcal{C} \cap \mathcal{P} \) 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, \( \mathcal{C} \), on the lines are 2-SC(4,6,2). If those two lines are non \( i \)-lines then \( \mathcal{C} \cup \{0\} \) 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\((n,2d+1,2)\). Further, \( \mathcal{A} \cup \{0\} \) is a 2-SC\((n,2d+1+1,2)\).

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** Let \( P \) 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

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

$$= \frac{3^n - 2^{n+1} + 1}{2}.$$ 

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 example, 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 $PG(5,2)$.

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

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 0. If, for any two vectors $x, y \in \mathcal{F}$, $|\text{supp}(x) \cap \text{supp}(y)| \geq 1$, then $\mathcal{F}$ is $i$-line free.
The proof is seen in [9].

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

**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**


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