A General Formula of the (t, n)-Threshold Visual Secret Sharing Scheme

Hiroki Koga

Faculty of Engineering Mechanics and Systems,
University of Tsukuba
1-1-1 Tennoudai, Tsukuba-shi, Ibaraki 305-8573, Japan
koga@esys.tsukuba.ac.jp

Abstract. This paper provides a new method for construction of the generating (or basis) matrices of the (t, n)-threshold visual secret sharing scheme ((t, n)-VSSS) for any $n \geq 2$ and $2 \leq t \leq n$. We show that there exists a bijection between a set of generating matrices of the (t, n)-VSSS and a set of homogeneous polynomials of degree n satisfying a certain property. We also show that the set of homogeneous polynomials is identified with a set of lattice points in a linear space of dimension $n - t + 1$ with explicitly expressed bases. These results yields a general formula of the generating matrices of the (t, n)-VSSS. The formula is not only theoretically of interest but also enables us to obtain efficient generating matrices that have been unknown.

1 Introduction

The visual secret sharing scheme (VSSS) is a new paradigm of the secret sharing proposed by Naor and Shamir [14]. Letting $\mathcal{P} = \{1, 2, \ldots, n\}$ be a set of participants, in the VSSS a black-white secret image is encrypted to n black-white images called shares. The VSSS has a property that, while a qualified set of participants can reproduce a secret image only by stacking all of their shares, a forbidden subset of participants can obtain no information on the secret image from their shares. If every $S \subseteq \mathcal{P}$ with $|S| \geq t$ is qualified and every $S \subset \mathcal{P}$ with $|S| \leq t-1$ is forbidden for some $2 \leq t \leq n$, we call such a VSSS the (t, n)-VSSS, where $|S|$ denotes the cardinality of S.

In this paper we focus on the (t, n)-VSSS. Literatures on the (t, n)-VSSS for black-white images can be classified into the following categories:

1. Construction of the optimal $(n.n)$-VSSS: [14].
2. Construction of the optimal (t, n)-VSSS in a certain class: [2] (for $t = 2$), [3] (for $t = 3, 4, 5, n-1$).
3. Developing algorithms to find a non-optimal (t, n)-VSSS without optimality: [6],[9].
4. Giving examples of (t, n)-VSSS: [4], [5],[12],[13],[14].
5. Introducing another notion of optimality: [1], [7],[15].
6. Formulating the problem of finding the optimal (t, n)-VSSS as a linear programming problem: [3], [8],[11].

Here, the optimality of the (t, n)-VSSS is usually defined in terms of the clearness of the reproduced secret image obtained by stacking arbitrary t shares. In the literature above, however, the most important and fascinating problem of finding the optimal (t, n)-VSSS for arbitrary $n \geq 2$ and $2 \leq t \leq n$ still remains unsolved.

The (t, n)-VSSS is realized by using a pair of matrices (X_0, X_1) called generating matrices (though (X_0, X_1) is sometimes called basis matrices, we use a different terminology in order to avoid confusion). In this paper we propose a simple method for obtaining pairs of generating matrices of the (t, n)-VSSS that is valid for all $n \geq 2$ and $2 \leq t \leq n$. The polynomial representation of generating matrices, which was first proposed by [10] and was extended by [12, 13], gives a key to the method. We show that a pair of generating matrices in a certain class can be identified with a lattice point in a linear space of homogeneous polynomials of dimension $n - t + 1$. More precisely, letting $e_{t,n}^{(i)}, i = 0, 1, \ldots, n - t$, be the bases of the linear space, for each $(\beta_0, \beta_1, \ldots, \beta_{n-t}) \in \mathcal{B}_{n-t+1}$, where $\mathcal{B}_{n-t+1}$ is the collection of all $(\beta_0, \beta_1, \ldots, \beta_{n-t})$ satisfying $\beta_i \in \mathbf{Z}$ for all $i = 0, 1, \ldots, n - t$ and $\sum_{i=0}^{n-t} \beta_i > 0$, we can identify $f = \sum_{i=0}^{n-t} e_{t,n}^{(i)}$ as a pair of generating matrices. In addition, if we apply a simple operation to such f, we can obtain more efficient pair of generating matrices each of which belongs to a class of matrices that is often treated.

We can use the proposed method for obtaining suboptimal pairs of generating matrices. The optimality can be defined in arbitrary sense, that is, we can maximize the relative difference [14] or minimize the number of subpixels. We have only to consider a finite subset $\mathcal{B}'_{n-t+1} \subset \mathcal{B}_{n-t+1}$ and exhaustively search for a pair of generating matrices in $\mathcal{B}'_{n-t+1}$ that is the most desirable. We checked that this search is realistic if $n \leq 9$ and found interesting examples of the (t, n)-VSSS that have been unknown.

This paper is organized as follows. In Section 2 we first define the (t, n)-VSSS mathematically. Then, we introduce important classes of matrices called column-permuting matrices (CPMs) [10] and different permuting matrices (DPMs) [12]. We explain several properties on concatenations of CPMs or DPMs. Section 3 is devoted to description of main results of this paper. We first show that there exists a bijection from the pairs of matrices realizing the (t, n)-VSSS to the set of homogeneous polynomials of degree n satisfying a certain property. We next show that for any $n \geq 2$ and $2 \leq t \leq n$ such homogeneous polynomials are regarded as lattice points of a linear space of dimension $n - t + 1$. These results mean that, surprisingly, any one of such lattice points yields a pair of generating matrices of the (t, n)-VSSS. We also give suboptimal pairs of generating matrices of the (t, n)-VSSS obtained for all $n \leq 9$ that was found by computer search.

2 Visual Secret Sharing Scheme

2.1 Definition of the Visual Secret Sharing Scheme

Let $\mathcal{P} = \{1, 2, \ldots, n\}$ be a set of participants, where $n \geq 2$. Denote the set composed by all the subsets of $\mathcal{P}$ by $2^{\mathcal{P}}$. Given an $n \times m$ Boolean matrix X

and an $S \in 2^{\mathcal{P}}$, we define $X[S]$ as the $|S| \times m$ matrix that is the restriction of X to the rows specified by S. The "or" of all the rows in $X[S]$ is denoted by $\mathrm{OR}(X[S])$. In addition, the Hamming weight of $\mathrm{OR}(X[S])$ is denoted by $h(\mathrm{OR}(X[S]))$. Letting t be an arbitrary integer satisfying $2 \le t \le n$, we define the (t, n)-threshold visual secret sharing scheme ((t, n)-VSSS for short) in the following way:

Definition 1 (Naor and Shamir [14]). *Let $\mathcal{C}_0$ and $\mathcal{C}_1$ be collections of $n \times m$ matrices. We say that a pair $(\mathcal{C}_0, \mathcal{C}_1)$ forms the (t, n)-VSSS if $(\mathcal{C}_0, \mathcal{C}_1)$ satisfies both of the following two conditions:*

1. *There exist constants $d > 0$ and $\alpha > 0$ satisfying:*
   (a) For any $S \in 2^{\mathcal{P}}$ with $|S| = t$, $h(\mathrm{OR}(X[S])) \le d - \alpha m$ for all $X \in \mathcal{C}_0$.
   (b) For any $S \in 2^{\mathcal{P}}$ with $|S| = t$, $h(\mathrm{OR}(X[S])) \ge d$ for all $X \in \mathcal{C}_1$.
2. *For an $S \in 2^{\mathcal{P}}$ and $i = 0, 1$ define $\mathcal{D}_i[S]$ as the collection of $X[S]$, $X \in \mathcal{C}_i$. Then, for any $S \in 2^{\mathcal{P}}$ with $|S| < t$ $\mathcal{D}_0[S]$ and $\mathcal{D}_1[S]$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.*

A secret image, which is assumed to be a black-white image, is encrypted into n images called *shares* in the following way. In fact, every pixel in a secret image is encrypted as m pixels called *subpixels* in each share. We first choose an element $X \in \mathcal{C}_0$ ($X \in \mathcal{C}_1$) randomly with uniform distribution if a pixel to be encrypted is white (black). Then, for $i = 1, 2, \ldots, n$ we encrypt the pixel as the m subpixels specified by the i-th row of X. This encryption is repeated until all the pixels in a secret image are encrypted. We assume that the i-th share is distributed to the participant i for $i = 1, 2, \ldots, n$.

Condition 1-(a) in Definition 1 guarantees that for any $S \in 2^{\mathcal{P}}$ with $|S| = t$ a black-white secret image is reproduced only by stacking all of the shares specified by S. When we stack arbitrary t shares in an arbitrary order, we can perceive a gap of the Hamming weights more than αm consisting in stacked m subpixels. That is, the m stacked subpixels corresponding to a white pixel in the secret image look brighter than the m stacked subpixels corresponding to a black pixel. Here, the parameter α is called the *relative difference* [14]. In general, the greater α becomes, the clearer we can perceive the secret image. On the other hand, condition 2 in Definition 1 means that no information on the secret image is revealed from the shares specified by S for any $S \in 2^{\mathcal{P}}$ with $|S| \le t - 1$. In fact, if $|S| \le t - 1$, the participants in S can obtain no information on the color of a pixel because both $\mathcal{D}_0[S]$ and $\mathcal{D}_1[S]$ contain $X[S]$ with the same frequencies.

It is often that $\mathcal{C}_0$ and $\mathcal{C}_1$ are constructed from all the permutations of rows of two matrices X_0 and X_1. We call such matrices the *generating matrices*. Though such matrices are sometimes called the basis matrices rather than the generating matrices [2, 3], we call (X_0, X_1) a pair of generating matrices in this paper because we use the term "basis" for expressing a different, but an ordinary, notion. Throughout this paper we consider construction of the (t, n)-VSSS using a pair of generating matrices. See [14] for examples of generating matrices.

2.2 Polynomial Representation of Generator Matrices

Hereafter, we consider the generating matrices that belong to a certain class. We define two classes of matrices called the column-permuting matrices (CPMs) [10] and the different permuting matrices (DPMs) [12].

Consider a Boolean vector $V = [v_1, v_2, \ldots, v_n]^T$ with n components, where the superscript T denotes the transpose. We can obtain $n!$ vectors from all the permutations (permitting multiplicity) of components of V. The $n \times n!$ matrix $M_n(v_1, v_2, \ldots, v_n)$ containing all of such $n!$ vectors as rows is called a column-permuting matrix (CPM) of order n [10]. For the case of $n = 3$ and $V = [0, 0, 1]^T$, $M_3(0, 0, 1)$ can be expressed as

$$M_3(0,0,1) = \begin{bmatrix} 0\,0\,1\,0\,1\,0 \\ 0\,0\,0\,1\,0\,1 \\ 1\,1\,0\,0\,0\,0 \end{bmatrix}. \tag{1}$$

(In order to avoid confusion, readers may consider $M_3(v_1, v_2, v_3)$ with distinct v_1, v_2 and v_3 and set $v_1 = 0$, $v_2 = 0$ and $v_3 = 1$.) We regard two CPMs as identical if an adequate permutation of rows of one equals to the other. We represent the CPM obtained from a vector with k 1's and $n - k$ 0's as the monomial $a^{n-k}z^k$, where a and z are the symbols corresponding to 0 and 1, respectively. For example, $M_3(0, 0, 1)$ in (1) is represented as a^2z.

Next, we consider concatenations of CPMs. Letting $M_n(u_1, u_2, \ldots, u_n)$ and $M_n(v_1, v_2, \ldots, v_n)$ be two CPMs with $v_i, u_i \in \{0, 1\}$ for all $i = 1, 2, \ldots, n$, we denote the concatenation of $M_n(u_1, u_2, \ldots, u_n)$ and $M_n(v_1, v_2, \ldots, v_n)$ by $M_n(u_1, u_2, \ldots, u_n) \odot M_n(v_1, v_2, \ldots, v_n)$. Here, we regard $M_n(u_1, u_2, \ldots, u_n) \odot M_n(v_1, v_2, \ldots, v_n)$ as the $n \times (2n!)$ matrix containing all the permutations (permitting multiplicity) of two Boolean vectors $[u_1, u_2, \ldots, u_n]^T$ and $[v_1, v_2, \ldots, v_n]^T$. We regard two concatenations of CPMs as identical if an adequate permutation of rows of one equals the other. Letting $[u_1, u_2, \ldots, u_n]^T$ be a Boolean vector with k 1's and $n - k$ 0's and $[v_1, v_2, \ldots, v_n]^T$ a Boolean vector with l 1's and $n - l$ 0's, we represent $M_n(u_1, u_2, \ldots, u_n) \odot M_n(v_1, v_2, \ldots, v_n)$ as the polynomial $a^{n-k}z^k + a^{n-l}z^l$. That is, the concatenation of matrices is represented by using $+$ in the polynomial representation. In particular, for the case of $k = l$ we express $a^{n-k}z^k + a^{n-k}z^k$ as $2a^{n-k}z^k$ for short. Obviously, any concatenation of CPMs of order n is represented as a homogeneous polynomial of a and z of degree n. In addition, it is important to notice that two concatenations of CPMs are identical if and only if the polynomial representation of one is equal to the other in the ordinary sense. For example, a concatenation of CPMs $M_3(0, 0, 0) \odot M_3(0, 1, 1) \odot M_3(0, 1, 1) \odot M_3(1, 1, 1)$, which is represented as $a^3 + 2az^2 + z^3$, is identical with another concatenation of CPMs $M_3(0, 1, 1) \odot M_3(1, 1, 1) \odot M_3(0, 1, 1) \odot M_3(0, 0, 0)$ that also has the polynomial representation $az^2 + z^3 + az^2 + a^3 = a^3 + 2az^2 + z^3$.

It is important to notice that we can represent the operation in which we eliminate an arbitrary row from a CPM $M_n(v_1, v_2, \ldots, v_n)$ as application of the partial differential operator $\psi \stackrel{\text{def}}{=} \frac{\partial}{\partial a} + \frac{\partial}{\partial z}$ to the polynomial representation of

$M_n(v_1, v_2, \ldots, v_n)$. For example, if we eliminate the the third row of $M_3(0,0,1)$ in (1), we have $M_2(0,0) \odot M_2(0,1) \odot M_2(0,1)$. This operation is represented as $\psi(a^2z) = a^2 + 2az$ in the polynomial representation. The definition of the CPM guarantees that we can obtain the same matrix if we eliminate either the first row or the second row instead of the third row. In the same way, the operation eliminating j arbitrary rows from a CPM is represented as application of ψ to its polynomial representation repeatedly for j times. The repeated application of ψ for j times is denoted by ψ^j. It is obvious that the same property on the elimination of rows also holds for concatenations of CPMs.

Next, we define the different permuting matrix (DPM). While [3, 6, 9] use different terminology for the same class of matrices, we follow the terminology given in [12]. Consider a Boolean vector $V = [v_1, v_2, \ldots, v_n]^T$. Suppose that V contains k 1's and $n-k$ 0's as its components. Then, we can obtain $\binom{n}{k}$ different vectors from all the permutations of components of V. The $n \times \binom{n}{k}$ matrix containing all of such $\binom{n}{k}$ vectors as rows is called a different permuting matrix (DPM) of order n and is denoted by $N_n(v_1, v_2, \ldots, v_n)$. For the case of $n = 3$, $N_3(0,0,0)$ and $N_3(0,0,1)$ are written as

$$N_3(0,0,0) = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \quad \text{and} \quad N_3(0,0,1) = \begin{bmatrix} 1\,0\,0 \\ 0\,1\,0 \\ 0\,0\,1 \end{bmatrix}. \tag{2}$$

It is important to notice that $M_3(0,0,1)$ in (1) satisfies $M_3(0,0,1) = N_3(0,0,1) \odot N_3(0,0,1)$ (recall that rows of $M_3(0,0,1)$ can be permuted adequately). More generally, for $[v_1, v_2, \ldots, v_n]^T$ containing k 1's and $n-k$ 0's, it is easy to verify that $M_n(v_1, v_2, \ldots, v_n)$ is the concatenation of $(n-k)!k!$ $N_n(v_1, v_2, \ldots, v_n)$'s. This motivates us to represent $N_n(v_1, v_2, \ldots, v_n)$ as the monomial $\frac{a^{n-k}z^k}{(n-k)!k!}$ [12]. In particular, for the cases of $k = 0$ and $k = n$ we use the representations $\frac{a^n}{n!}$ and $\frac{z^n}{n!}$, respectively. We also use $+$ for denoting concatenation of DPMs. Then, it obviously follows that eliminating an arbitrary row from a DPM is represented as application of $\psi = \frac{\partial}{\partial a} + \frac{\partial}{\partial z}$ to the monomial representation of the DPM. In fact, if we eliminate the third row from $N_3(0,0,1)$, which is represented as $\frac{a^2z}{2!1!}$, we have the concatenation of DPMs represented as $\psi(\frac{a^2z}{2!1!}) = az + \frac{a^2}{2!}$. In addition, eliminating j arbitrary rows from a DPM is represented as application of ψ^j to its monomial representation. It is obvious that the same property on the elimination of rows holds for concatenations of DPMs.

Now, we introduce the following four sets of homogeneous polynomials:

$$\mathcal{H}_n = \left\{ \sum_{i=0}^{n} \gamma_i a^{n-i} z^i \;:\; \gamma_i \in \mathbf{Z} \text{ for all } i = 0, 1, \ldots n \right\}, \tag{3}$$

$$\mathcal{H}_n^+ = \left\{ \sum_{i=0}^{n} \gamma_i a^{n-i} z^i \;:\; \gamma_i \in \mathbf{Z} \text{ and } \gamma_i > 0 \text{ for all } i = 0, 1, \ldots n \right\}, \tag{4}$$

$$\mathcal{K}_n = \left\{ \sum_{i=0}^{n} \gamma_i \frac{a^{n-i} z^i}{(n-i)!i!} \;:\; \gamma_i \in \mathbf{Z} \text{ for all } i = 0, 1, \ldots n \right\}, \tag{5}$$

$$\mathcal{K}_n^+ = \left\{ \sum_{i=0}^{n} \gamma_i \frac{a^{n-i} z^i}{(n-i)!i!} \,:\, \gamma_i \in \mathbf{Z} \text{ and } \gamma_i > 0 \text{ for all } i = 0, 1, \ldots n \right\}, \tag{6}$$

where $\mathbf{Z}$ denotes the set of all integers. Then, as summary, we have the following proposition.

Proposition 1. *(a) Any concatenation of CPMs (DPMs) of order n is expressed as an element in $\mathcal{H}_n^+$ ($\mathcal{K}_n^+$). Conversely, any element in $\mathcal{H}_n^+$ ($\mathcal{K}_n^+$) is interpreted as a concatenation of CPMs (DPMs) of order n.*
(b) Let X be any concatenation of CPMs (DPMs) with the polynomial representation $f \in \mathcal{H}_n^+$ ($f \in \mathcal{K}_n^+$). Then, for any $1 \le j \le n-1$ the polynomial representation of the matrix obtained by eliminating arbitrary j rows from X is given by $\psi^j f$.

Then, we have the following theorem. While the primary version of Theorem 1-(a) was given by Koga, Iwamoto and Yamamoto [10] for the (t, n)-VSSS of color images, Kuwakado and Tanaka [12] pointed out that Theorem 1-(b) holds for the case of (t, n)-VSSS of black-white images. Proof of Theorem 1 is given in Appendix A for readers' convenience.

Theorem 1. *(a) Suppose that $f_0 \in \mathcal{H}_n^+$ and $f_1 \in \mathcal{H}_n^+$ satisfy*

$$\psi^{n-t+1} f_0 = \psi^{n-t+1} f_1 \tag{7}$$

and

$$\psi^{n-t} f_0|_{z=0} = C_0 a^t, \quad \psi^{n-t} f_1|_{z=0} = C_1 a^t \tag{8}$$

for some nonnegative integers C_0 and C_1 with $C_0 > C_1$. Define X_0 and X_1 as the concatenations of CPMs with the polynomial expressions f_0 and f_1, respectively. Then, (X_0, X_1) becomes a pair of generating matrices of the (t, n)-VSSS.
(b) Suppose that $g_0 \in \mathcal{K}_n^+$ and $g_1 \in \mathcal{K}_n^+$ satisfy

$$\psi^{n-t+1} g_0 = \psi^{n-t+1} g_1 \tag{9}$$

and

$$\psi^{n-t} g_0|_{z=0} = C_0 \frac{a^t}{t!}, \quad \psi^{n-t} g_1|_{z=0} = C_1 \frac{a^t}{t!} \tag{10}$$

for some nonnegative integers C_0 and C_1 with $C_0 > C_1$. Define X_0 and X_1 as the concatenations of DPMs with the polynomial expressions g_0 and g_1, respectively. Then, (X_0, X_1) becomes a pair of generating matrices of the (t, n)-VSSS.

We conclude this section with introducing two more notions. First, we define the decomposition of an element in $\mathcal{H}_n$ or $\mathcal{K}_n$. If an $f \in \mathcal{H}_n$ is written as $f = f^+ - f^-$, where f^+ and f^- belong to $\mathcal{H}_n^+ \cup \{0\}$ and f^+ and f^- contain no term in common, we call $f = f^+ - f^-$ the *decomposition* of f. For example, if $f = a^2 z - az^2 + z^3 \in \mathcal{H}_3$, we have $f^+ = a^2 z + z^3$ and $f^- = az^2$. Note that the decomposition is unique and f^+ (f^-) equals zero if all the terms in f have negative (positive) coefficients. The decomposition of $g \in \mathcal{K}_n$ is defined in the same way. That is, if $g = \frac{a^3}{3!} - \frac{a^2 z}{2!1!} + 2\frac{z^3}{3!} \in \mathcal{K}_3$, we have $g^+ = \frac{a^3}{3!} + 2\frac{z^3}{3!}$ and $g^- = \frac{a^2 z}{2!1!}$. Next, we define the *norm* of $f \in \mathcal{H}_n$. Suppose that f is expressed as $f = \sum_{i=0}^{n} \gamma_i a^{n-i} z^i$. Then, the norm $||f||$ of f is defined by $||f|| = \sum_{i=0}^{n} |\gamma_i|$, where $|\gamma_i|$ denotes the absolute value of γ_i. Clearly, $||f|| \geq 0$ for all $f \in \mathcal{H}_n$ and $||f|| = 0$ if and only if $f = 0$. It is clear that for the matrix X with a polynomial expression $f \in \mathcal{H}_n^+$, $||f||$ means the number of CPMs contained in X.

3 Main Results

3.1 Characterization of the (t, n)-VSSS as a Vector Space

Theorem 1-(a) guarantees that, if we can find $f_0 \in \mathcal{H}_n^+$ and $f_1 \in \mathcal{H}_n^+$ satisfying (7) and (8), we obtain a pair of generating matrices (X_0, X_1) of the (t, n)-VSSS, where X_0 and X_1 are the concatenations of CPMs corresponding to f_0 and f_1, respectively. However, Theorem 1 does not tell us at all how we can find such f_0 and f_1. Since ψ^{n-t+1} and ψ^{n-t} are linear, the homogeneous polynomial $f \in \mathcal{H}_n$ defined by $f = f_0 - f_1$ satisfies $\psi^{n-t+1} f = 0$ and $\psi^{n-t} f|_{z=0} = Ca^t$ for some integer $C > 0$. This motivates us to define the following subsets of $\mathcal{H}_n$ and $\mathcal{K}_n$:

$$\mathcal{F}_{t,n} = \{f \in \mathcal{H}_n \,:\, \psi^{n-t+1} f = 0 \text{ and } \psi^{n-t} f|_{z=0} = Ca^t \text{ for some integer } C > 0\},$$
$$\mathcal{G}_{t,n} = \{g \in \mathcal{K}_n \,:\, \psi^{n-t+1} g = 0 \text{ and } \psi^{n-t} g|_{z=0} = C\tfrac{a^t}{t!} \text{ for some integer } C > 0\}.$$

We also define the sets of pairs of matrices by

$$\mathcal{M}_{t,n} = \{(X_0, X_1) \,:\, X_0 \text{ and } X_1 \text{ satisfy all of } (\mathrm{A}_1), (\mathrm{B}_1), (\mathrm{C}_1), (\mathrm{D}_1)\},$$
$$\mathcal{N}_{t,n} = \{(X_0, X_1) \,:\, X_0 \text{ and } X_1 \text{ satisfy all of } (\mathrm{A}_2), (\mathrm{B}_2), (\mathrm{C}_1), (\mathrm{D}_1)\},$$

where conditions (A_1), (A_2), (B_1), (B_2), (C_1) and (D_1) are given as follows:

- (A_1) both X_0 and X_1 are concatenations of CPMs,
- (A_2) both X_0 and X_1 are concatenations of DPMs,
- (B_1) X_0 and X_1 contain no CPM in common,
- (B_2) X_0 and X_1 contain no DPM in common,
- (C_1) $X_0[S] = X_1[S]$ for any $S \in 2^{\mathcal{P}}$ with $|S| = t - 1$, where the equality $X_0[S] = X_1[S]$ is interpreted in the sense that $X_1[S]$ coincides $X_0[S]$ by an adequate permutation of rows,
- (D_1) $h(\mathrm{OR}(X_0[S])) < h(\mathrm{OR}(X_1[S]))$ for any $S \in 2^{\mathcal{P}}$ with $|S| = t$, where $h(\cdot)$ denotes the Hamming weight.

That is, $\mathcal{M}_{t,n}$ ($\mathcal{N}_{t,n}$) is the set of all the pairs of generating matrices obtained by concatenations of CPMs (DPMs) containing no CPM (DPM) in common. Then, we have the following theorem that is a stronger version of Theorem 1.

Theorem 2. *For any $n \geq 2$ and $2 \leq t \leq n$, there exist bijections $\varphi : \mathcal{M}_{t,n} \to \mathcal{F}_{t,n}$ and $\sigma : \mathcal{N}_{t,n} \to \mathcal{G}_{t,n}$.*

Proof. We only prove the existence of a bijection $\varphi : \mathcal{M}_{t,n} \to \mathcal{F}_{t,n}$ below because the existence of $\sigma : \mathcal{N}_{t,n} \to \mathcal{G}_{t,n}$ can be proved in the same way.

Suppose that $(X_0, X_1) \in \mathcal{M}_{t,n}$. Since X_0 and X_1 are assumed to be concatenations of CPMs, Proposition 1 guarantees that there exist unique $f_0 \in \mathcal{H}_n^+$ and $f_1 \in \mathcal{H}_n^+$ corresponding to X_0 and X_1, respectively. In addition, we note that the converse of Theorem 1 is also true. That is, such f_0 and f_1 satisfy (7) and (8). We define f by $f = f_0 - f_1$. Clearly, f belongs to $\mathcal{H}_n$ and satisfies

$$\psi^{n-t+1} f = 0 \quad \text{and} \quad \psi^{n-t} f|_{z=0} = (C_1 - C_2)a^t \tag{11}$$

due to the linearity of ψ^{n-t+1} and ψ^{n-t}. Since $C_1 > C_2$ from Definition 1 and the definitions of f_0, f_1 and f, (11) guarantees that $f \in \mathcal{F}_{t,n}$. We define φ as the mapping that maps a pair $(X_0, X_1) \in \mathcal{M}_{t,n}$ to $f = f_0 - f_1 \in \mathcal{F}_{t,n}$, where f_0 and f_1 are the polynomial representations of X_0 and X_1, respectively.

First, we prove that φ is one-to-one. Assume that $(X_0, X_1) \in \mathcal{M}_{t,n}$ and $(\tilde{X}_0, \tilde{X}_1) \in \mathcal{M}_{t,n}$ satisfy $\varphi(X_0, X_1) = \varphi(\tilde{X}_0, \tilde{X}_1)$. Let $f_0, f_1, \tilde{f}_0$ and $\tilde{f}_1$ be the polynomial expressions of $X_0, X_1, \tilde{X}_0$ and $\tilde{X}_1$, respectively. Note that, since $(X_0, X_1) \in \mathcal{M}_{t,n}$, f_0 and f_1 contain no term in common due to the definition of $\mathcal{M}_{t,n}$. Similarly, $\tilde{f}_0$ and $\tilde{f}_1$ contain no term in common as well. It is important to notice that $\varphi(X_0, X_1) = \varphi(\tilde{X}_0, \tilde{X}_1)$ means that $f_0 - f_1 = \tilde{f}_0 - \tilde{f}_1$, i.e.,

$$f_0 - \tilde{f}_0 = f_1 - \tilde{f}_1. \tag{12}$$

Now, define h by $h = f_0 - \tilde{f}_0$. Clearly, $h \in \mathcal{H}_n$ because both f_0 and $\tilde{f}_0$ belong to $\mathcal{H}_n$. Denoting the decomposition of h by $h = h^+ - h^-$, (12) leads to

$$\begin{cases} f_0 + h^- = \tilde{f}_0 + h^+, \\ f_1 + h^- = \tilde{f}_1 + h^+. \end{cases} \tag{13}$$

Since h^+ and h^- contain no term in common due to the definition of the decomposition, (13) means that both f_0 and f_1 contain h^+ in common. This implies that $h^+ = 0$ because f_0 and f_1 contain no term in common by assumption. Similarly, we obtain $h^- = 0$, and therefore, we have $h = 0$. By combining $h = 0$ with (12), we have $f_0 - f_1 = \tilde{f}_0 - \tilde{f}_1$, i.e., $(X_0, X_1) = (\tilde{X}_0, \tilde{X}_1)$, which shows that φ is one-to-one.

Next, we prove that φ is onto. To this end, fix an $f \in \mathcal{F}_{t,n}$ arbitrarily. Then, it holds that $\psi^{n-t+1} f = 0$ and $\psi^{n-t} f|_{z=0} = Ca^t$ for some integer $C > 0$. Letting $f = f^+ - f^-$ be the decomposition of f, it follows that $\psi^{n-t+1} f^+ = \psi^{n-t+1} f^-$ and

$$\psi^{n-t} f|_{z=0} = \psi^{n-t} f^+|_{z=0} - \psi^{n-t} f^-|_{z=0} = Ca^t \tag{14}$$

owing to the linearity of ψ^{n-t+1} and ψ^{n-t}. In addition, since f^+ and f^- belong to $\mathcal{H}_n^+ \cup \{0\}$, there exist integers $C_0 \geq 0$ and $C_1 \geq 0$ such that $\psi^{n-t} f^+|_{z=0} = C_0 a^t$ and $\psi^{n-t} f^-|_{z=0} = C_1 a^t$. In view of (14), C_0 and C_1 satisfy $C_0 = C_1 + C > C_1$. Therefore, by virtue of Theorem 1-(a), the pair of matrices (X_0, X_1) corresponding to (f^+, f^-) satisfies $(X_0, X_1) \in \mathcal{M}_{t,n}$. $\square$

Since Theorem 2 guarantees the existence of a bijection $\varphi : \mathcal{M}_{t,n} \to \mathcal{F}_{t,n}$, we can know more about $\mathcal{M}_{t,n}$ by developing properties of $\mathcal{F}_{t,n}$. The following lemma characterizes a key property of a set including $\mathcal{F}_{t,n}$.

Lemma 1. *Define*

$$\mathcal{E}_{t,n} = \left\{ f \in \mathcal{R}_n \,:\, \psi^{n-t+1} f = 0 \right\}, \tag{15}$$

where

$$\mathcal{R}_n = \left\{ \sum_{i=0}^{n} \gamma_i a^{n-i} z^i \,:\, \gamma_i \in \mathbf{R} \right\}$$

and $\mathbf{R}$ *denotes the set of all real numbers. Then,* $\mathcal{E}_{t,n}$ *is a linear space of dimension* $n-t+1$ *with bases*

$$e_{t,n}^{(i)} = a^{n-t-i} z^i (a-z)^t, \quad i = 0, 1, \ldots, n-t. \tag{16}$$

Proof. Clearly, the linearity of ψ^{n-t+1} implies that $\mathcal{E}_{t,n}$ is a linear space. We prove both $\dim \mathcal{E}_{t,n} \geq n-t+1$ and $\dim \mathcal{E}_{t,n} \leq n-t+1$, where $\dim \mathcal{E}_{t,n}$ denotes the dimension of $\mathcal{E}_{t,n}$. We can see that $e_{t,n}^{(i)}$, $0 \leq i \leq n-t$, form bases of $\mathcal{E}_{t,n}$ from the proof below.

First, we prove $\dim \mathcal{E}_{t,n} \geq n-t+1$. We use the formula similar to the Leibniz formula

$$\psi^k(fg) = \sum_{j=0}^{k} \binom{k}{j} (\psi^{k-j} f)(\psi^j g) \tag{17}$$

for all $k \geq 1$ and infinitely differentiable f and g, which can be easily proved by induction on k. Letting i an arbitrary integer with $0 \leq i \leq n-t$, it follows from (17) that

$$\begin{aligned} \psi^{n-t+1} e_{t,n}^{(i)} &= \psi^{n-t+1} \left(a^{n-t-i} z^i (a-z)^t \right) \\ &= \sum_{j=0}^{n-t+1} \binom{n-t+1}{j} \left(\psi^{n-t+1-j} (a^{n-t-i} z^i) \right) \left(\psi^j (a-z)^t \right). \end{aligned} \tag{18}$$

By noticing that $\psi^j (a-z)^t = 0$ for all $j \geq 1$, (18) leads to

$$\psi^{n-t+1} e_{t,n}^{(i)} = \left[\psi^{n-t+1} \left(a^{n-t-i} z^i \right) \right] (a-z)^t = 0 \tag{19}$$

where the last equality in (19) follows because $\psi^{n-t+1} f = 0$ for any $f \in \mathcal{R}_k$ with $k < n-t+1$. Hence, we have $\psi^{n-t+1} e_{t,n}^{(i)} = 0$ for all $i = 0, 1, \ldots, n-t$.

We can verify that $e_{t,n}^{(i)}$, $0 \leq i \leq n-t$, are linearly independent in the following way. Assume that there exist real numbers $\beta_0, \beta_1, \ldots, \beta_{n-t}$ satisfying

$$\sum_{i=0}^{n-t} \beta_i e_{t,n}^{(i)} = 0. \tag{20}$$

We notice that the greatest degree with respect to a on the left-hand side of (20) is at most n and a term including a^n appears only in $e_{t,n}^{(0)}$. This means that $\beta_0 = 0$. By repeating this argument, we have $\beta_0 = \beta_1 = \cdots = \beta_{n-t} = 0$. Hence, it turns out that $e_{t,n}^{(i)}$, $0 \le i \le n-t$, are linearly independent. Consequently, we have established that $\dim \mathcal{E}_{t,n} \ge n-t+1$.

Next, we prove $\dim \mathcal{E}_{t,n} \le n-t+1$. We prove that any $f \in \mathcal{E}_{t,n}$ can be expressed as a linear combination of $e_{t,n}^{(i)}$, $0 \le i \le n-t$. To this end, fix

$$f = \sum_{i=0}^{n} \gamma_i a^{n-i} z^i \in \mathcal{E}_{t,n} \tag{21}$$

arbitrarily, where $\gamma_i \in \mathbf{R}$ for all $i = 0, 1, \ldots, n-t$. Then, since among the bases $e_{t,n}^{(i)}$, $0 \le i \le n-t$, the term including a^n is contained only in $e_{t,n}^{(0)}$ and the coefficient of such a term in $e_{t,n}^{(0)}$ is equal to 1, f can be written as

$$f = \gamma_0 e_{t,n}^{(0)} + \left(\sum_{i=1}^{n} \gamma_i a^{n-i} z^i - \gamma_0 e_{t,n}^{(0)} \right). \tag{22}$$

Notice that the greatest degree with respect to a of the second term in (22) is at most $n-1$. That is, we can rewrite (22) in the following form:

$$f = \gamma_0 e_{t,n}^{(0)} + \sum_{i=1}^{n} \gamma_i' a^{n-i} z^i, \tag{23}$$

where γ_i, $1 \le i \le n$, are constants determined from γ_i, $1 \le i \le n-t$, and $e_{t,n}^{(0)}$. By repeating this argument, we next have

$$f = \gamma_0 e_{t,n}^{(0)} + \gamma_1' e_{t,n}^{(1)} + \sum_{i=2}^{n} \gamma_i'' a^{n-i} z^i, \tag{24}$$

and finally have

$$f = \sum_{i=0}^{n-t} \tilde{\gamma}_i e_{t,n}^{(i)} + g, \tag{25}$$

where $\tilde{\gamma}_i$, $0 \le i \le n-t$, are constants, $g = z^{n-t+1} h$ and $h \in \mathcal{R}_{t-1}$. Here, we use the following lemma that is proved in Appendix B.

Lemma 2. *Let l be an arbitrary integer satisfying $0 \le l \le n$. If $g \in \mathcal{R}_n$ can be written as $g = z^l h$ for some $h \in \mathcal{R}_{n-l}$ and satisfies $\psi^l g = 0$, then $g = 0$.*

Since it holds that $\psi^{n-t+1} f = 0$ and $\psi^{n-t+1} e_{t,n}^{(i)} = 0$ for all $i = 0, 1, \ldots, n-t$, (25) implies that $\psi^{n-t+1} g = 0$. By applying Lemma 2 to g in (25), we have $g = 0$. This completes the proof of $\dim \mathcal{E}_{t,n} \le n-t+1$. $\square$

Now, we are ready to give the following theorem that characterizes $\mathcal{F}_{t,n}$ as lattice points.

Theorem 3. *For any $n \geq 2$ and $2 \leq t \leq n$, it holds that*

$$\mathcal{F}_{t,n} = \left\{ \sum_{i=0}^{n-t} \beta_i e_{t,n}^{(i)} \,:\, \beta_i \in \mathbf{Z} \text{ for all } i = 0, 1, \ldots, n-t \text{ and } \sum_{i=0}^{n-t} \beta_i > 0 \right\}. \quad (26)$$

Proof. We use the fact that $e_{t,n}^{(i)}$, $0 \leq i \leq n-t$, satisfy $\psi^{n-t} e_{t,n}^{(i)} = (n-t)!(a-z)^t$ and therefore

$$\psi^{n-t} e_{t,n}^{(i)}|_{z=0} = (n-t)!\, a^t \quad \text{for all } i = 0, 1, \ldots, n-t, \quad (27)$$

which can be easily verified similarly to the method that develops $\psi^{n-t+1} e_{t,n}^{(i)} = 0$ in (18) and (19). Let $\mathcal{L}_{t,n}$ denote the set on the right-hand side of (26). We prove Theorem 3 by developing both $\mathcal{F}_{t,n} \subseteq \mathcal{L}_{t,n}$ and $\mathcal{L}_{t,n} \subseteq \mathcal{F}_{t,n}$. Since $\mathcal{F}_{t,n} \subset \mathcal{E}_{t,n}$, an arbitrary $f \in \mathcal{F}_{t,n}$ can be expressed as

$$f = \sum_{i=0}^{n-t} \beta_i e_{t,n}^{(i)} + g \quad (28)$$

by using the same method that yields (25), where $g = z^{n-t+1} h$ and $h \in \mathcal{R}_{t-1}$. If we apply Lemma 2 to g in (28), we have $g = 0$. In addition, it is important to notice that $\beta_i \in \mathbf{Z}$ for all $i = 0, 1, \ldots, n-t$ because no division is included in the method. By applying ψ^{n-t} to both sides of (28) and set $z = 0$, we have

$$\psi^{n-t} f|_{z=0} = (n-t)! \left(\sum_{i=0}^{n-t} \beta_i \right) a^t \quad (29)$$

from (27). Since $f \in \mathcal{F}_{t,n}$ satisfies $\psi^{n-t} f|_{z=0} = Ca^t$ for some integer $C > 0$, (29) implies that $\sum_{i=0}^{n-t} \beta_i > 0$. This establishes $\mathcal{F}_{t,n} \subseteq \mathcal{L}_{t,n}$.

Proof of $\mathcal{L}_{t,n} \subseteq \mathcal{F}_{t,n}$ is easy. Fix an $f \in \mathcal{L}_{t,n}$ arbitrarily. Since $f \in \mathcal{L}_{t,n}$, f is expressed as $f = \sum_{i=0}^{n-t} \beta_i e_{t,n}^{(i)}$, where $\beta_i \in \mathbf{Z}$ for all $i = 0, 1, \ldots, n-t$ and $\sum_{i=0}^{n-t} \beta_i > 0$. Then, it immediately follows from Lemma 1, (27) and the linearity of ψ^{n-t+1} and ψ^{n-t} that

$$\psi^{n-t+1} f = \sum_{i=0}^{n-t} \beta_i (\psi^{n-t+1} e_{t,n}^{(i)}) = \sum_{i=0}^{n-t} \beta_i \cdot 0 = 0, \quad (30)$$

$$\psi^{n-t} f|_{z=0} = \sum_{i=0}^{n-t} \beta_i (\psi^{n-t} e_{t,n}^{(i)})|_{z=0} = (n-t)! \left(\sum_{i=0}^{n-t} \beta_i \right) a^t, \quad (31)$$

which shows that $f \in \mathcal{F}_{t,n}$ because $\sum_{i=0}^{n-t} \beta_i > 0$ by assumption. □

Now, define

$$\mathcal{B}_k = \left\{ (\beta_0, \beta_1, \ldots, \beta_{k-1}) \in \mathbf{Z}^k \,:\, \sum_{i=0}^{k-1} \beta_i > 0 \right\}. \quad (32)$$

for $k \geq 1$. Then, Theorem 3 tells us that each $(\beta_0, \beta_1, \ldots, \beta_{n-t}) \in \mathcal{B}_{n-t+1}$ gives an element of $f \in \mathcal{F}_{t,n}$. Since Theorem 2 guarantees that there exists a bijection $\varphi : \mathcal{M}_{t,n} \to \mathcal{F}_{t,n}$, such that $f \in \mathcal{F}_{t,n}$ yields a pair of generating matrices $\varphi^{-1}(f) = (X_0, X_1) \in \mathcal{M}_{t,n}$. The following corollary describes properties of such a pair of generating matrices.

Corollary 1. *Let $(\beta_0, \beta_1, \ldots, \beta_{n-t}) \in \mathcal{B}_{n-t+1}$ be arbitrarily given. Let $(X_0, X_1) \in \mathcal{M}_{t,n}$ be the pair of generating matrices corresponding to $f = \sum_{i=0}^{n-t} \beta_i e_{t,n}^{(i)} \in \mathcal{F}_{t,n}$. Then, the relative difference α of (X_0, X_1) is given by*

$$\alpha = 2\sum_{i=0}^{n-t} \beta_i \Bigg/ \left[\binom{n}{t} ||f||\right], \tag{33}$$

where $||f||$ denotes the norm of f. In addition, the number of rows in X_0 (or X_1) is equal to $||f|| \cdot n!/2$.

Proof. Recall that $\psi^{n-t} f|_{z=0}$ is given by (31) for any $f = \sum_{i=0}^{n-t} \beta_i e_{t,n}^{(i)} \in \mathcal{F}_{t,n}$. Equation (31) means that the relative difference of the pair of generating matrices $\varphi^{-1}(f) = (X_0, X_1)$ is caused by $(n-t)! \left(\sum_{i=0}^{n-t} \beta_i\right)$ CPMs each of which is represented as a^t. Since the CPM represented as a^t contains $t!$ 0's, the number of subpixels yielding relative difference is equal to $W = (n-t)!t! \sum_{i=0}^{n-t} \beta_i$.

Next, we evaluate the number of rows contained in X_0 or X_1. Recall that, letting $f = f^+ - f^-$ be the decomposition of f, X_0 and X_1 have the polynomial representations f^+ and f^-, respectively. Clearly, we have $||f|| = ||f^+|| + ||f^-||$. In addition, since $f = \sum_{i=0}^{n-t} \beta_i e_{t,n}^{(i)}$ and $e_{t,n}^{(i)}|_{a=z=1} = 0$ for all $i = 0, 1, \ldots, n-t$, setting $a = z = 1$ in $f = f^+ - f^-$ leads to $||f^+|| = ||f^-||$. Hence, it holds that $||f^+|| = ||f^-|| = ||f||/2$. Since both X_0 and X_1 are concatenations of $||f^+|| = ||f^-||$ CPMs each of which has $n!$ rows, the number of rows M of X_0 and X_1 turns out to satisfy $M = ||f|| \cdot n!/2$. Then, the claim of the corollary is immediate because $\alpha = W/M$. □

We have developed a method which enables us to construct a pair of generating matrix $(X_0, X_1) \in \mathcal{M}_{t,n}$ from an $f \in \mathcal{F}_{t,n}$. In fact, letting f be an arbitrary element of $\mathcal{F}_{t,n}$ and $f = f^+ - f^-$ the decomposition of f, X_0 and X_1 are concatenations of CPMs with the polynomial representations f^+ and f^-, respectively. However, Corollary 1 tells us that the number of rows of such X_0 and X_1 can be large because they have $||f|| \cdot n!/2$ rows.

However, we can also develop a method for finding a pair of generating matrices with less number of rows. We make use of the fact that any CPM can be written as a concatenation of DPMs. To this end, we define

$$\mathcal{G}_{t,n}^* = \left\{ \sum_{i=0}^{n} \gamma_i \frac{a^{n-i} z^i}{(n-i)!i!} \in \mathcal{G}_{t,n} \,:\, \gcd\{\gamma_i \,:\, i = 0, 1, \ldots, n-t\} = 1 \right\}, \tag{34}$$

where $\gcd\{\gamma_i : i = 0, 1, \ldots, n-t\}$ denotes the greatest common divisor ≥ 1. In order to reduce the number of rows, we use the mapping $\pi : \mathcal{F}_{t,n} \to \mathcal{G}_{t,n}^*$ given in the following proposition.

Proposition 2. *For any $n \geq 2$ and $2 \leq t \leq n$ there exists a surjection $\pi : \mathcal{F}_{t,n} \to \mathcal{G}^*_{t,n}$.*

Proof. We define π in the following way. Let $f = \sum_{i=0}^{n} \gamma_i a^{n-i} z^i$ be an arbitrary element in $\mathcal{F}_{t,n}$. Since for each $i = 0, 1, \ldots, n$ the CPM with the monomial representation $a^{n-i}z^i$ is concatenation of $(n-i)!i!$ DPMs with the monomial representation $\frac{a^{n-i}z^i}{(n-i)!i!}$, f can be written as

$$f = \sum_{i=0}^{n} \gamma_i (n-i)!i! \frac{a^{n-i}z^i}{(n-i)!i!}. \tag{35}$$

Define G by $G = \gcd\{\gamma_i(n-i)!i! : i = 0, 1, \ldots, n-t\}$. Then, we can define $\pi : \mathcal{F}_{t,n} \to \mathcal{G}^*_{t,n}$ as $\pi : f \mapsto \sum_{i=0}^{n} \frac{\gamma_i(n-i)!i!}{G} \frac{a^{n-i}z^i}{(n-i)!i!}$. It is easy that this π is surjective. $\square$

We call the operation converting $f \in \mathcal{F}_{t,n}$ into $\pi(f) \in \mathcal{G}^*_{t,n}$ the *contraction*. Notice that Theorem 2-(b) guarantees that $(Y_0, Y_1) \stackrel{\text{def}}{=} \sigma^{-1}(\pi(f))$ becomes a pair of generating matrices of the (t, n)-VSSS. Obviously, while the relative difference caused by (Y_0, Y_1) is the same as that of (X_0, X_1), the number of rows of Y_i becomes $1/G$ times as X_i for $i = 0, 1$. Summarizing, we have the following theorem giving a general formula of the (t, n)-VSSS:

Theorem 4. *Let $n \geq 2$ and $2 \leq t \leq n$ be arbitrary integers. Then, for each $(\beta_0, \beta_1, \ldots, \beta_{n-t}) \in \mathcal{B}_{n-t+1}$, $f = \sum_{i=0}^{n-t} \beta_i e^{(i)}_{t,n}$ leads to a pair of the generating matrices $(Y_0, Y_1) = \sigma^{-1}(\pi(f)) \in \mathcal{N}_{t,n}$. The relative difference α and the number of rows M of such a (Y_0, Y_1) is given by (33) and $M = ||f|| \cdot n!/(2G)$, respectively, where, letting $f = \sum_{i=0}^{n} \gamma_i a^{n-i} z^i$ denote the expansion of f, G is defined by $G = \gcd\{\gamma_i(n-i)!i! : i = 0, 1, \ldots, n\}$.*

Example 1. We construct a pair of generating matrices (Y_0, Y_1) for the $(3, 4)$-VSSS by using Theorem 4. Theorem 4 tells us that for each $(\beta_0, \beta_1) \in \mathcal{B}_2$ $f = \beta_0 a(a-z)^3 + \beta_1 z(a-z)^3$ yields $(Y_0, Y_1) \in \mathcal{N}_{3,4}$. If we set $(\beta_0, \beta_1) = (1, 1)$, it easily follows that

$$\begin{aligned} f &= a(a-z)^3 + z(a-z)^3 \\ &= a^4 - 2a^3z + 2az^3 - z^4 \\ &= 4!\frac{a^4}{4!} - 2 \cdot 3!\frac{a^3z}{3!1!} + 2 \cdot 3!\frac{az^3}{1!3!} - 4!\frac{z^4}{4!} \\ &= 2 \cdot 3!\left[2\frac{a^4}{4!} - \frac{a^3z}{3!1!} + \frac{az^3}{1!3!} - 2\frac{z^4}{4!}\right], \end{aligned} \tag{36}$$

which means that $g \stackrel{\text{def}}{=} \pi(f) = 2\frac{a^4}{4!} - \frac{a^3z}{3!1!} + \frac{az^3}{1!3!} - 2\frac{z^4}{4!}$. Since the decomposition of g is given by $g^+ = 2\frac{a^4}{4!} + \frac{az^3}{1!3!}$ and $g^- = \frac{a^3z}{3!1!} + 2\frac{z^4}{4!}$, the concatenations of DPMs corresponding to g^+ and g^- become Y_0 and Y_1 respectively. By using

Proposition 1-(a) we obtain

$$Y_0 = \begin{bmatrix} 0\,0\,0\,1\,1\,1 \\ 0\,0\,1\,0\,1\,1 \\ 0\,0\,1\,1\,0\,1 \\ 0\,0\,1\,1\,1\,0 \end{bmatrix} \quad \text{and} \quad Y_1 = \begin{bmatrix} 1\,1\,1\,0\,0\,0 \\ 1\,1\,0\,1\,0\,0 \\ 1\,1\,0\,0\,1\,0 \\ 1\,1\,0\,0\,0\,1 \end{bmatrix}.$$

This pair of generating matrices, which yields $\alpha = 1/6$, coincides with the pair of generating matrices of the $(3, n)$-VSSS given by Naor and Shamir [14] with $n = 4$. Recall that (Y_0, Y_1) is heuristically constructed in [14]. □

Notice that the converse of Theorem 4 is also true. That is, we can show that for any $(Y_0, Y_1) \in \mathcal{N}_{t,n}$ there exists an $f \in \mathcal{F}_{t,n}$ satisfying $(Y_0, Y_1) = \sigma^{-1}(\pi(f))$. This property is due to the fact that $\pi : \mathcal{F}_{t,n} \to \mathcal{G}^*_{t,n}$ is surjective and there exists a surjection $\tilde{\pi} : \mathcal{G}_{t,n} \to \mathcal{G}^*_{t,n}$ which is defined similarly to π in Proposition 2.

3.2 Construction of Suboptimal (t, n)-VSSS Using the Formula

In this subsection we consider construction of an optimal (t, n)-VSSS by using Theorem 4. We consider the following two kinds of criteria for optimization: (A) maximization of the relative difference α, and (B) minimization of the number of rows M. If there exist more than one pair of generating matrices with maximum α under (A), we choose the pair with the smallest M. On the other hand, if there exist more than one pair of generating matrices with minimum M under (B), we choose the pair of with the greatest α.

How can we find the optimal $(Y_0, Y_1) \in \mathcal{N}_{t,n}$ by using Theorem 4 under criteria (A) or (B)? Unfortunately, it is quite difficult to find the optimal (Y_0, Y_1) theoretically because the formulas of α and M given in Theorem 4 include $||f||$ or G. However, we can use Theorem 4 in the following way for finding a suboptimal pair of generating matrices of (t, n)-VSSS. We first choose a subset $\mathcal{B}'_{n-t+1} \subset \mathcal{B}_{n-t+1}$ with a finite number of elements adequately. Next, for each $(\beta_0, \beta_1, \ldots, \beta_{n-t}) \in \mathcal{B}'_{n-t+1}$ we expand $f = \sum_{i=0}^{n-t} \beta_i e^{(i)}_{t,n}$ to the form $f = \sum_{i=0}^{n} \gamma_i a^{n-i} z^i$ and compute $G = \gcd\{\gamma_i (n-i)! i! \,:\, i = 0, 1, \ldots, n\}$. Since Theorem 4 tells us that both M and α are determined from f and G, recalling that $|\mathcal{B}'_{n-t+1}| < \infty$, we can find $(\beta_0, \beta_1, \ldots, \beta_{n-t}) \in \mathcal{B}'_{n-t+1}$ that leads to $(Y_0, Y_1) \in \mathcal{N}_{t,n}$ optimal in $\mathcal{B}'_{n-t+1}$. Though we mention only (A) and (B) as criteria of optimization here, such a search is possible under another criterion given in [7, 15]. In addition, notice that, since $\mathcal{B}_{n-t+1}$ is a countably infinite set, we can choose $\mathcal{B}'_{n-t+1}$ such that the suboptimal (Y_0, Y_1) becomes globally optimal as $|\mathcal{B}'_{n-t+1}| \to \infty$.

In our computer search, we defined $\mathcal{B}'_{n-t+1}$ as the collection of all $(\beta_0, \beta_1, \ldots, \beta_{n-t}) \in \mathbf{Z}^{n-t+1}$ satisfying $\beta_i \geq 0$ for all $i = 0, 1, \ldots, n-t$, $\gcd\{\beta_0, \beta_1, \ldots, \beta_{n-t}\} = 1$ and $\sum_{i=0}^{n-t} \beta_i \leq 120$. For each $n \leq 9$ and $2 \leq t \leq n-1$ we exhaustively searched for $(\beta_0, \beta_1, \ldots, \beta_{n-t}) \in \mathcal{B}'_{n-t+1}$ that yields $(Y_0, Y_1) \in \mathcal{N}_{t,n}$ with the optimality in $\mathcal{B}'_{n-t+1}$ under the two respective criteria. Clearly, time required for this search becomes long as $n - t + 1$ increases. However, for small n such as 9 this search

Table 1. Suboptimal (t, n)-VSSS in $\mathcal{B}'_{n-t+1}$ for $3 \le n \le 9$ under (A)

(t,n)	M	α	$\{\beta_i\}_{i=0}^{n-t}$
(2,3)	3	$\frac{1}{3}$	$\{1,2\},\{2,1\}$
(2,4)	6	$\frac{1}{3}$	$\{1,2,1\}$
(3,4)	6	$\frac{1}{6}$	$\{1,1\}$
(2,5)	10	$\frac{3}{10}$	$\{2,4,6,3\}$, $\{3,6,4,2\}$
(3,5)	8	$\frac{1}{8}$	$\{3,4,3\}$
(4,5)	15	$\frac{1}{15}$	$\{2,3\},\{3,2\}$
(2,6)	20	$\frac{3}{10}$	$\{1,2,3,2,1\}$
(3,6)	10	$\frac{1}{10}$	$\{2,3,3,2\}$
(4,6)	36	$\frac{1}{18}$	$\{4,7,4\}$
(5,6)	30	$\frac{1}{30}$	$\{1,1\}$
(2,7)	35	$\frac{2}{7}$	$\{3,6,9,12,8,4\}$, $\{4,8,12,9,6,3\}$
(3,7)	30	$\frac{1}{10}$	$\{3,9,11,9,3\}$
(4,7)	70	$\frac{3}{70}$	$\{15,32,38,20\}$, $\{20,38,32,15\}$

(t,n)	M	α	$\{\beta_i\}_{i=0}^{n-t}$
(5,7)	48	$\frac{1}{48}$	$\{2,3,2\}$
(6,7)	70	$\frac{1}{70}$	$\{3,4\},\{4,3\}$
(2,8)	70	$\frac{2}{7}$	$\{1,2,3,4,3,2,1\}$
(3,8)	42	$\frac{2}{21}$	$\{1,3,4,4,3,1\}$
(4,8)	160	$\frac{3}{80}$	$\{9,20,26,20,9\}$
(5,8)	112	$\frac{1}{56}$	$\{2,5,5,2\}$
(6,8)	198	$\frac{1}{99}$	$\{15,26,15\}$
(7,8)	140	$\frac{1}{140}$	$\{1,1\}$
(2,9)	126	$\frac{5}{18}$	$\{4,8,12,16,20,15,10,5\}$, $\{5,10,15,20,16,12,8,4\}$
(3,9)	56	$\frac{5}{56}$	$\{5,15,21,23,21,15,5\}$
(4,9)	630	$\frac{2}{63}$	$\{3,7,10,10,7,3\}$
(5,9)	8064	$\frac{13}{896}$	$\{11,29,37,29,11\}$
(6,9)	1764	$\frac{1}{147}$	$\{19,39,37,17\}$
(7,9)	252	$\frac{1}{252}$	$\{1,2,1\}$
(8,9)	315	$\frac{1}{315}$	$\{4,5\},\{5,4\}$

was completed in realistic time (at most several days) when we used a personal computer with a Pentium III 1.0GHz processor.

Table 1 shows M and α of generation matrices of (t, n)-VSSS that is optimal in $\mathcal{B}'_{n-t+1}$ under criterion (A). While [3] discusses the optimality on α for $t = 3, 4, 5, n-1$ from a combinatoric viewpoint under (A), their approach cannot be applied to the cases of $6 \le t \le n-2$. We found pairs of generating matrices of $(6, 8)$-, $(6, 9)$- and $(7, 9)$-VSSSs with the optimality (A) in $\mathcal{B}'_{n-t+1}$. For each $2 \le n \le 9$ and $2 \le t \le 4$, α in Table 1 attains the theoretical upper bound given in [8] from linear programming approach (for $t \ge 5$ no upper bound is given in [8]). In addition, for each $2 \le n \le 9$ and $2 \le t \le 5$ α in Table 1 is greater than or equal to α in [5] except for the case of $(5, 7)$-VSSS (for $t \ge 6$ α is not written in [5]). The pair of generating matrices of the $(5, 7)$-VSSS in [5], yielding $\alpha = 4/147$, may not belong to $\mathcal{N}_{t,n}$ because we cannot find such a pair even from a larger set $\{(\beta_0, \beta_1, \beta_2) \in \mathbf{Z}^3 : \beta_0 + \beta_1 + \beta_2 > 0, |\beta_i| \le 1000$ for i=0,1,2$\}$. Furthermore, a pair of generating matrices of the $(4, 7)$-VSSS, which is written as $g = 15\frac{a^7}{7!} - 4\frac{a^6 z}{6!1!} + \frac{a^3 z^4}{3!4!} - 6\frac{az^6}{1!6!} + 20\frac{z^7}{7!}$ in the polynomial expression and was first reported in [12], was turned out to be optimal in $\mathcal{B}'_{n-t+1}$ (the method for finding such g is not written in [12]). Clearly, this pair of generating matrices, yielding $\alpha = 3/70$ and $M = 70$, is better than the pair given by [3] with $\alpha = 3/80$ and $M = 160$.

On the other hand, if $n \leq 9$, under (B) we found pairs of generating matrices (Y_0, Y_1) with the same number of rows as the pairs given by Droste [6] except for the case of $(6,8)$-VSSS. While Droste [6] mentions the existence of (Y_0, Y_1) with $M = 128$ and $\alpha = 1/128$, we found (Y_0, Y_1) with $M = 126$ and $\alpha = 1/126$ (choose $(\beta_0, \beta_1, \beta_2) = (5, 14, 9)$ or $(9, 14, 5)$). In addition, for the case of $n = 10$, we found a pair of generating matrices of the $(8,10)$-VSSS with $M = 590$ and $\alpha = 1/590$ (choose $(\beta_0, \beta_1, \beta_2) = (14, 22, 9)$), though Droste [6] just mentions the existence of (Y_0, Y_1) with $M = 640$ and $\alpha = 1/640$.

It is also interesting to find a $(\beta_0, \beta_1, \ldots, \beta_{n-t}) \in \mathcal{B}_{n-t+1}$ that lead to a simple pair of generating matrices $(Y_0, Y_1) \in \mathcal{N}_{t,n}$. We conclude the paper by giving such a (Y_0, Y_1) expressed in the polynomial representation for $t = n, n-1, 2$

(i) (n,n)-VSSS

Theorem 3 tells us that elements of $\mathcal{F}_{n,n}$ can be written as $f = \beta_0(a-z)^n$, where β_0 is a positive integer. Then, it easily follows that

$$\begin{aligned} f &= \beta_0 \sum_{i=0}^{n} (-1)^i \binom{n}{i} a^{n-i} z^i \\ &= \beta_0 n! \left[\sum_{i=0}^{n} (-1)^i \frac{a^{n-i} z^i}{(n-i)!i!} \right] \end{aligned}$$

Hence, we have $\pi(f) = \sum_{i=0}^{n} (-1)^i \frac{a^{n-i}z^i}{(n-i)!i!}$ that is independent of β_0. This is a pair of generating matrices with $\alpha = 1/2^n$ given by Naor and Shamir [14].

(ii) $(n-1,n)$-VSSS

Theorem 3 guarantees that $f \in \mathcal{F}_{n-1,n}$ can be expressed as $f = \beta_0 a(a-z)^{n-1} + \beta_1 z(a-z)^{n-1}$, where $(\beta_0, \beta_1) \in \mathcal{B}_2$. We set $\beta_0 = \beta_1 = 1$ for even n and $\beta_0 = \lfloor \frac{n}{2} \rfloor$ and $\beta_1 = \lceil \frac{n}{2} \rceil$ for odd n. Then, $\pi(f)$ can be expressed as

$$\pi(f) = \begin{cases} \displaystyle\sum_{i=0}^{n} (-1)^i \left(\frac{n}{2} - i \right) \frac{a^{n-i} z^i}{(n-i)!i!}, & \text{if } n \text{ is even}, \\ \displaystyle\sum_{i=0}^{n} (-1)^i \left(\frac{n+1}{2} - i \right) \frac{a^{n-i} z^i}{(n-i)!i!}, & \text{if } n \text{ is odd}, \end{cases}$$

which leads to the pair of generating matrices with $M = \frac{n}{2}\binom{n-1}{n/2-1}$ and $\alpha = 1/[\frac{n}{2}\binom{n-1}{n/2-1}]$ for even n and $M = n\binom{n-1}{(n-1)/2}$ and $\alpha = 4/[n\binom{n-1}{(n-1)/2}]$ for odd n. These pairs of generating matrices are given by Blundo et al [3].

(iii) $(2,n)$-VSSS

By Theorem 3, $f \in \mathcal{F}_{2,n}$ can be written as $f = \sum_{i=0}^{n-2} \beta_i a^{n-2-i} z^i (a-z)^2$, where $(\beta_0, \beta_1, \ldots, \beta_{n-2}) \in \mathcal{B}_{n-1}$. If we set $\beta_i = n-1-i$ for all $i = 0, 1, \ldots, n-2$, we have

$$\pi(f) = (n-1)\frac{a^n}{n!} - \frac{a^{n-1}z}{(n-1)!1!} + \frac{z^n}{n!},$$

which leads to the pair of generating matrices given by Naor and Shamir [14] with $M = n$ and $\alpha = 1/n$. On the other hand, for the case of even n if we set $\beta_i = i + 1$ for $i = 0, 1, \ldots, \frac{n}{2} - 1$ and $\beta_i = n - i - 1$ for $i = \frac{n}{2}, \frac{n}{2} + 1, \ldots, n - 2$, we have

$$\pi(f) = \frac{1}{2}\binom{n}{n/2}\frac{a^n}{n!} - \frac{a^{n/2}z^{n/2}}{(n/2)!(n/2)!} + \frac{1}{2}\binom{n}{n/2}\frac{z^n}{n!},$$

The pair of generating matrices corresponding to f above satisfies $M = \binom{n}{n/2}$ and $\alpha = \frac{n}{4(n-1)}$.

Appendix:

A Proof of Theorem 1

We prove Theorem 1-(a) here because Theorem 1-(b) can be developed similarly. Let X_0 and X_1 be concatenations of CPMs with the polynomial representations f_0 and f_1, respectively. By the assumption of the theorem, f_0 and f_1 satisfy (7) and (8). In view of Definition 1 and the definition of the generating matrices, it is sufficient to prove that (i) $X_0[S] = X_1[S]$ for any $S \in 2^{\mathcal{P}}$ with $|S| = t-1$, and (ii) $h(\mathrm{OR}(X_0[S])) < h(\mathrm{OR}(X_1[S]))$ for any $S \in 2^{\mathcal{P}}$ with $|S| = t$.

The proof of property (i) is simple. Since Proposition 1 tells us that for $i = 0, 1$ application of ψ^{n-t+1} to f_i means elimination of arbitrary $n-t+1$ rows from X_i, (7) implies that $X_0[S] = X_1[S]$ for any $S \in 2^{\mathcal{P}}$ with $|S| = t-1$. This establishes property (i). On the other hand, we notice that $\psi^{n-t} f_i|_{z=0}$ means the number of the CPMs represented as a^t in $\mathrm{OR}(X_i[S])$ for any $S \in 2^{\mathcal{P}}$ with $|S| = t$. Then, (8) implies that $\mathrm{OR}(X_0[S])$ contains the CPMs represented as a^t more than $\mathrm{OR}(X_1[S])$, which immediately leads to $h(\mathrm{OR}(X_0[S])) < h(\mathrm{OR}(X_1[S]))$. This establishes property (ii).

B Proof of Lemma 2

We prove Lemma 2 by induction on l. The claim of the lemma is trivial if $l = 0$. Let $l \geq 1$ be an arbitrary integer and suppose that an arbitrary $g \in \mathcal{R}_n$ with $g = z^l h$ for some $h \in \mathcal{R}_{n-l}$ satisfies $\psi^l g = 0$. Since

$$\begin{aligned}\psi^l g &= \psi^l(z^l h) \\ &= \psi^{l-1}\left(\{lh + z\cdot(\psi h)\}z^{l-1}\right),\end{aligned} \tag{B.1}$$

we have

$$lh + z\cdot(\psi h) = 0 \tag{B.2}$$

by induction hypothesis. Setting

$$h = \gamma_0 a^{n-l} + \gamma_1 a^{n-l-1}z + \cdots + \gamma_{n-l}z^{n-l},$$

(B.2) leads to

$$l\gamma_0 a^{n-l}+[(n-l)\gamma_0+2\gamma_1]a^{n-l-1}z+\cdots+[\gamma_{n-l-1}+(n-l+1)\gamma_{n-l}]z^{n-l}=0, \quad \text{(B.3)}$$

which mean that $l\gamma_0 = (n-l)\gamma_0 + 2\gamma_1 = \cdots = \gamma_{n-l-1} + (n-l+1)\gamma_{n-l} = 0$ and therefore $\gamma_0 = \gamma_1 = \cdots = \gamma_{n-l} = 0$.

References

1. C. Blundo and A. De Santis, "Visual cryptography schemes with perfect reconstruction of black pixels," *Computer and Graphics*, vol. 22, no. 4, pp. 449-455, 1998.
2. C. Blundo, A. De Santis and D. R. Stinson, "On the contrast in visual cryptography schemes," *Journal of Cryptology*, vol. 12, no. 4, pp. 261-289, 1999.
3. C. Blundo, P. D'Arco, A. De Santis and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," submitted to *SIAM Journal on Discrete Mathematics*. (Available from `http://cacr.math.uwaterloo.ca/~dstinson`)
4. C. Blundo, A. De Bonis, and A. De Santis, "Improved schemes for visual cryptography," *Designs, Codes, and Cryptography*, vol. 24, pp. 255–278, 2001.
5. C. K. Choi, S. S. Yang, J. H. Park and R. Kohno, "New construction for improving contrast in visual cryptography," *Proc. of ISITA*, Mexico City, pp. 368–371, 1998.
6. S. Droste, "New results on visual cryptography," *Advance in Cryptography-CRYPT'96*, LNCS 1109, pp. 401–415, Springer Verlag, 1996.
7. P. A. Eisen and D. R. Stinson, "Threshold visual cryptography scheme with specified whiteness levels of reconstructed pixels," *Designs, Codes, and Cryptology*, vol. 25, No. 1, pp. 15–61, 2002.
8. T. Hofmeister, M. Krause and H. U. Simon, "Contrast-optimal k out of n secret sharing schemes in visual cryptography," *Theoretical Computer Science*, vol. 240, pp. 471–485, 2000.
9. T. Kato and H. Imai, "An extended construction method of visual secret sharing scheme," *IEICE Trans.*, vol. J79-A, no. 8, pp. 1344–1351, 1996. (in Japanese)
10. H. Koga, M. Iwamoto and H. Yamamoto, "An analytic construction of the visual sercet sharing scheme for color images," *IEICE Trans. on Fundamentals*, vol. E84-A, no. 1, pp. 262–272, 2001.
11. M. Krause and H. U. Simon, "Determining the optimal contrast for secret sharing in visual cryptography," *Latin 2000*, LNCS 1776, pp. 280–291, 2000.
12. H. Kuwakado and H. Tanaka, "Polynomial represenation of visual secret sharing scheme for black-white images," *Proc. of 2001 Symposium on Cryptography and Information Security*, pp. 417–422, 2001.
13. H. Kuwakado and H. Tanaka, "Polynomial represenation of visual secret sharing scheme and its application," *IEICE Trans. on Fundamentals*, vol. E85-A, no. 6, pp. 1379–1386, 2002.
14. M. Naor and A. Shamir, "Visual cryptography," *Advance in Cryptography-EUROCRYPT'94*, LNCS 950, pp. 1–12, Springer-Verlag, 1994.
15. E. R. Verheul and H. C. A. van Tilborg, "Constructions and properties of k out of n visual secret sharing schemes," *Designs, Codes, and Cryptography*, vol. 11, no. 2, pp. 179 – 196, 1997.