Grey Level Visual Cryptography for General Access Structures

by

Lesley Anne MacPherson

A thesis

presented to the University of Waterloo

in fulfilment of the

thesis requirement for the degree of

Master of Mathematics

in

Computer Science

Waterloo, Ontario, Canada, 2002

Author's Declaration for Electronic Submission of a Thesis

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Visual cryptography, first introduced by Naor and Shamir, allows a secret (black and white) image to be encoded and distributed to a set of participants such that certain predefined sets of participants may reconstruct the image without any computation. In 2000, Blundo, De Santis, and Naor introduced a model for grey-level visual cryptography which is a generalization of visual cryptography for general access structures. Grey-level visual cryptography extends this model to include grey-scale images. Decoding is done by the human visual system.

In this thesis we survey known results of grey-level visual cryptography and visual cryptography for general access structures. We extend several visual cryptography constructions to grey-level visual cryptography, and derive new results on the minimum possible pixel expansion for all possible access structures on at most four participants.

Acknowledgements

Many thanks to my supervisor, Jeff Shallit, for his support and guidance in the writing process, and my reader Doug Stinson, for lending much of his time and expertise. Thanks also go to my other reader, Alfred Menezes, for his assistance.

I would also like to thank the National Science and Engineering Research Council for their financial assistance, without which this work would not have been possible.

Finally, thanks to my parents, Jeanne and Bruce MacPherson, for much love and encouragement, and most of all to Daniel Koch, for always being there.

Contents

List of Tables

Chapter 1

Introduction

Visual cryptography is a method of sharing a secret image among a group of participants, where certain groups of participants are defined as *qualified* and may combine their shares of the image to obtain the original, and certain other groups are defined as *forbidden* and even if they combine knowledge about their parts, cannot obtain any information on the secret image. The image is composed of black and white pixels. To encrypt, each pixel is divided into m subpixels, and for each pixel in the secret image, each participant is given m subpixels, some of which are black and some of which are white. These subpixels are so small that the eye averages them to some shade of grey. Each participant's share of the image can be thought of as a transparency with a mixture of black and white subpixels. To combine shares, participants simply stack their transparencies.

Visual cryptography is interesting because decryption requires no computation, but instead is done by the human visual system. The image reconstructed by combining shares of a qualified group of participants is not identical to the secret image. The pixels of the secret image that were white are a lighter shade of grey than the pixels of the image that were black, and the difference in the darkness of the black and white pixels is a parameter called *contrast.* Ideally, we want the contrast to be high so that it is easy to differentiate the black and white areas.

Originally, visual cryptography was restricted to black and white images. While black and white images are sufficient for data such as scanned text documents, black and white pictures are typically represented in grey scale. To represent these images, it is necessary to generalize the visual cryptography schemes (VCS) for black and white images to grey levels (GVCS, or grey level visual cryptography schemes). In grey level visual cryptography, there are a specified number of grey levels g. Each pixel is again divided into m subpixels which are either black or white. As in visual cryptography, these are so small that the human eye averages them to some shade of grey. The reconstructed image is not identical to the secret image. Each grey level, $0 \leq i < g$, corresponds to some range of shades of grey, with the lowest grey levels being the lightest and the highest grey levels the darkest. As in visual cryptography, there is a concept of contrast, but in grey level visual cryptography there is a set of contrast parameters corresponding to each adjacent pair of grey levels. Again, we want the contrast to be as large as possible, to make it easier to differentiate between two adjacent grey levels.

An *access structure* on a set of participants $\mathcal{P}$ is a pair of sets, one consisting of all qualified sets of participants and the other consisting of all forbidden sets of participants. The most common and significant type of access structure is what is known as a *threshold* access structure. Assuming that the total number of participants is n, a threshold structure is an access structure where any group of k or more participants is qualified and may reconstruct the secret, and any group of less than k participants is forbidden and has no information on the secret. These access structures are denoted as (k, n)-VCS ((k, n)-GVCS respectively). In this thesis, we will adapt a known technique for constructing an optimal (t, t)-VCS to construct an optimal (t, t)-GVCS. We will also extend a technique for constructing (k, n)-VCS (using an optimal (t, t)-VCS) to construct (k, n)-GVCS (Theorem 3.4).

While not as significant as threshold access structures, general access structures are also interesting. We will present two constructions for general access structures, both based on constructions for VCS. The first is called the cumulative array construction (Theorem 3.2), which utilizes a cumulative mapping and a (t, t)-threshold GVCS to construct the GVCS for the general access structure. The second is called the decomposition construction (Theorem 3.3). This construction breaks down the access structure into smaller access structures for which a GVCS is known, and combines the schemes to obtain a GVCS for the original access structure.

Finally, we will extend the results of Atienese, Blundo, De Santis, and Stinson [1], which give the optimal pixel expansion for access structures on four participants, to the GVCS model. In order to accomplish this, we will obtain a variety of theoretical results. We begin by showing that we do not need to consider access structures which are not connected (Theorem 4.4), that is, which can be considered as two separate access structures. We also do not need to consider access structures which contain isolated participants (Lemma 4.1), i.e., participants which can obtain the secret alone. We then prove some important results regarding unavoidable patterns, which are submatrices that must be present in the matrices of a GVCS for a given access structure. We use these to prove results about access structures which are based on graphs. The most significant result is one which gives the optimal pixel expansion for access structures arising from complete multipartite graphs (Theorem 4.16). We also use unavoidable patterns to give a lower bound on the pixel expansion for threshold access structures (Theorem 4.13). Finally, we give some special results on certain access structures (Theorem 4.17 and Theorem 4.18), and an upper bound for any GVCS for which a basis matrices construction is known for the corresponding VCS (Theorem 4.19).

Chapter 2

Background

2.1 Threshold VCS

Visual cryptography was first introduced by Naor and Shamir [6] in 1994. In their paper, they address the idea of visual cryptography for threshold structures. They assume that the image is composed of black and white pixels, and each pixel is encrypted separately. Each pixel of the image appears in the n shares distributed to the participants. It is divided into m *subpixels*, either black or white, which are sufficiently small and close that the eye averages them to some shade of grey. We can represent this with an $n \times m$ matrix: $S[i, j] = 1$ if and only if the j^{th} subpixel in the i^{th} share is black. When the shares are combined, the perceived grey level is proportional to the number of ones in the boolean OR of the m-vectors representing the shares of each participant.

The black and white areas of the image are determined by a rule of contrast based on three variables: a threshold value, a relative difference, and the number of subpixels (referred to as the *pixel expansion*). We use:

- t to denote the threshold value;
- α to denote the relative difference;
- m to denote the pixel expansion.

The *threshold value* is a numeric value for the point at which black areas are distinct from white. The value $\alpha \cdot m$ is the *contrast*, which we want to be as large as possible. We require that $\alpha \cdot m \geq 1$ to ensure that the black and white areas will be distinguishable.

We give the following definition of a threshold VCS, by Naor and Shamir [6]. The phrasing is taken directly from Atienese, Blundo, De Santis, and Stinson [1]. We use *OR* V to denote the boolean operation *OR* of a set of vectors with result V. The *Hamming weight* $w(V)$ is the sum of the elements in a boolean vector V (alternatively, the number of 1's in V).

Definition 2.1 A (k, n)-VCS consists of two collections of $n \times m$ matrices C_0 and C_1. To share a white (respectively black) pixel, the dealer randomly chooses one of the matrices in C_0 (C_1). The chosen matrix defines the color of the m subpixels in each of the n transparencies. The collections C_0 and C_1 must have the following properties:

1. For any $S \in C_0$, the *OR* V of any k of the n rows satisfies $w(V) \leq t - \alpha \cdot m$. Similarly, for any $S \in C_1$, the *OR* V of any k of the n rows satisfies $w(V) \geq t$.

2. For any subset $\{i_1, i_2, \ldots, i_q\}$ of $\{1, 2, \ldots, n\}$ with $q < k$, the two collections of $q \times m$ matrices D_t for $t \in \{0, 1\}$ obtained by restricting each $n \times m$ matrix in C_t to rows $i_1, i_2, \ldots, i_q$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

The first property of Definition 2.1 refers to the contrast of the scheme. The second refers to the security of the scheme, guaranteeing that if there are less than k parties, they will not be able to obtain any information on the secret image.

Naor and Shamir [6] also give a construction for a (k, k)-VCS which is optimal with respect to the pixel expansion m and prove its optimality. They construct the VCS as follows:

Consider a ground set $W = \{e_1, \ldots, e_k\}$ of k elements and let $\pi_1, \ldots, \pi_{2^{k-1}}$ be a list of all the subsets of W with even cardinality and let $\sigma_1, \ldots, \sigma_{2^{k-1}}$ be a list of all the subsets of W with odd cardinality. Each list defines the following $k \times 2^{k-1}$ matrices S_0 and S_1: For $1 \leq i \leq k$ and $1 \leq j \leq 2^{k-1}$, let $S_0[i][j] = 1$ iff $e_i \in \pi_j$ and $S_1[i][j] = 1$ iff $e_i \in \sigma_j$.

The collections C_0 and C_1 are obtained by permuting the columns of S_0 and S_1 in all possible ways. This scheme has $\alpha = 1/2^{k-1}$ and $m = 2^{k-1}$. Naor and Shamir go on to show that these values are optimal with respect to the pixel expansion for a (k, k)-VCS.

There is a simpler way to describe this construction. We can consider S_0 to consist of the boolean k-bit vectors with even Hamming weight and S_1 to consist of those with odd Hamming weight. Again, the collections C_0 and C_1 are obtained by permuting the columns of these matrices in all possible ways.

As in the above construction, it is frequently possible to use a single matrix to represent each collection, where the collection is generated by permuting the columns of the corresponding matrix in all possible ways. Such a matrix is called a *basis matrix*, and all the visual cryptography schemes we will be using in this thesis are represented using basis matrices. Basis matrices are advantageous because they are both easier to construct and provide a more concise representation of the scheme. In the optimal (k, k)-VCS construction above, S_0 and S_1 are the basis matrices. When discussing this construction we will generally refer to the basis matrices S_0 and S_1 instead of the collections C_0 and C_1.

2.2 VCS for General Access Structures

Research in visual cryptography has been largely focused on threshold access structures. However, general access structures are also interesting, and require a new definition of the model. We use the definition given by Atienese, Blundo, De Santis, and Stinson [1].

2.2.1 The model

Let $\mathcal{P} = \{1, \ldots, n\}$ be a set of n participants. Let $\Gamma_{\text{Qual}} \subseteq 2^{\mathcal{P}}$ be the set of *qualified* sets of participants, and $\Gamma_{\text{Forb}} \subseteq 2^{\mathcal{P}}$ be the set of *forbidden* sets of participants. Clearly we want $\Gamma_{\text{Qual}} \cap \Gamma_{\text{Forb}} = \emptyset$, as the same set of participants cannot be both qualified and forbidden. The pair $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ is called an *access structure* for $\mathcal{P}$. For $A \subseteq 2^{\mathcal{P}}$, we say that A is *monotone increasing* if for any $B \in A$ and any $C \subseteq \mathcal{P}$ such that $B \cap C = \emptyset$, we have $B \cup C \in A$. We say that A is *monotone decreasing* if for any $B \in A$ and any $C \subseteq B$ we have that $B \setminus C \in A$. In the case where Γ_{Qual} is monotone increasing, Γ_{Forb} is monotone decreasing, and $\Gamma_{\text{Qual}} \cup \Gamma_{\text{Forb}} = 2^{\mathcal{P}}$, we say the access structure is *strong.* We define $\Gamma_0 = \{A \in \Gamma_{\text{Qual}} : A' \notin \Gamma_{\text{Qual}} \ \forall A' \subset A\}$. We say that Γ_0 is a *basis.* In a strong access structure, Γ_{Qual} is the *closure* of Γ_0.

We also need to define essential and non-essential participants. A participant i is *essential* if there exists a set $X \subseteq \mathcal{P}$ such that $X \notin \Gamma_{\text{Qual}}$ but $X \cup \{i\} \in \Gamma_{\text{Qual}}$. We also say that i is *strongly essential* if $X \in \Gamma_{\text{Forb}}$ and $X \cup \{i\} \in \Gamma_{\text{Qual}}$. A participant i is *non-essential* if there does not exist a set X such that $X \notin \Gamma_{\text{Qual}}$ but $X \cup \{i\} \in \Gamma_{\text{Qual}}$.

We first define VCS in terms of collections of matrices. This definition is taken nearly verbatim from Atienese, Blundo, De Santis, and Stinson [1].

Definition 2.2 Let $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ be an access structure on n participants. The collections of $n \times m$ Boolean matrices C_0 and C_1 are a visual cryptography scheme with pixel expansion m if there exists values $\alpha(m)$ and sets $\{X, t_X\}_{X \in \Gamma_{\text{Qual}}}$ satisfying:

1. Any $X = \{j_1, \ldots, j_p\} \in \Gamma_{\text{Qual}}$ can recover the shared image by combining their shares. Formally, for any $M \in C_0$, the *OR* V of rows $j_1, \ldots, j_p$ satisfies $w(V) \leq t_X - \alpha(m) \cdot m$; whereas for any $M \in C_1$ we have that $w(V) \geq t_X$.

2. Any $X = \{j_1, \ldots, j_p\} \in \Gamma_{\text{Forb}}$ has no information on the shared image. Formally, the collections of $p \times m$ matrices D_0 and D_1 obtained by restricting each $n \times m$ matrix in C_0 and C_1 to rows $j_1, \ldots, j_p$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

As in Definition 2.1 the first property ensures that the participants will be able to distinguish the black and white pixels, and the second property ensures the security of the scheme.

Note that the threshold t in Definition 2.1 is the same for any choice of k participants. In Definition 2.2, we allow the threshold to vary with the choice of participants X and denote it by t_X.

Since all the constructions we will be working with use basis matrices, we will rewrite our definition in terms of basis matrices. When proving that a construction works, this is the definition we will refer to. This definition is also taken nearly verbatim from Atienese, Blundo, De Santis, and Stinson [1].

Definition 2.3 Let $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ be an access structure on n participants. The Boolean matrices S_0, S_1 are a visual cryptography scheme with pixel expansion m if there exists values $\alpha(m)$ and sets $\{X, t_X\}_{X \in \Gamma_{\text{Qual}}}$ satisfying:

1. If $X = \{j_1, \ldots, j_p\} \in \Gamma_{\text{Qual}}$ then the *OR* V of rows $j_1, \ldots, j_p$ of S_0 satisfies $w(V) \leq t_X - \alpha(m) \cdot m$; whereas for S_1 we have that $w(V) \geq t_X$.

2. If $X = \{j_1, \ldots, j_p\} \in \Gamma_{\text{Forb}}$ then the $p \times m$ matrices obtained by restricting S_0, S_1 to rows $j_1, \ldots, j_p$ are equal up to a column permutation.

We obtain the collections C_0, C_1 by permuting the columns of S_0, S_1 in all possible ways.

2.2.2 Constructions

Using this definition, Atienese, Blundo, De Santis, and Stinson [1] provide various constructions. Of particular interest are the cumulative arrays, decomposition, and starting matrices constructions.

A Cumulative Arrays Construction

Let $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ be a strong access structure on $\mathcal{P} = \{1, \ldots, n\}$, and let $Z_M = \{B \in \Gamma_{\text{Forb}} : B \cup \{i\} \in \Gamma_{\text{Qual}}\ \forall i \in \mathcal{P} \setminus B\}$ be the set of all maximal forbidden sets. Let $Z_M = \{F_0, \ldots, F_{t-1}\}$. The cumulative array is a $|\mathcal{P}| \times |Z_M|$ boolean matrix such that $CA[i,j] = 1$ if and only if $i \notin F_j$.

Let $\hat{S}_0$ and $\hat{S}_1$ be the basis matrices of a (t,t)-VCS. We use the cumulative array CA to construct the basis matrices S_0, S_1 from $\hat{S}_0$ and $\hat{S}_1$. For any fixed i let $j_{i,1}, \ldots, j_{i,g_i}$ be the integers j such that $CA[i,j] = 1$. The i^{th} row of S_0 (S_1 respectively) consists of the OR of rows $j_{i,1}, \ldots, j_{i,g_i}$ of $\hat{S}_0$ ($\hat{S}_1$ respectively).

A Decomposition Construction

The decomposition construction uses smaller access structures as building blocks for larger schemes. Let $(\Gamma'_{\text{Qual}}, \Gamma'_{\text{Forb}})$ and $(\Gamma''_{\text{Qual}}, \Gamma''_{\text{Forb}})$ be two access structures on a set of n participants $\mathcal{P}$. If a participant $i \in \mathcal{P}$ is non-essential for $(\Gamma'_{\text{Qual}}, \Gamma'_{\text{Forb}})$, we assume that $i \in \Gamma'_{\text{Forb}}$ and that i does not receive nothing as a share, and similarly for $(\Gamma''_{\text{Qual}}, \Gamma''_{\text{Forb}})$.

Suppose there exist a $(\Gamma'_{\text{Qual}}, \Gamma'_{\text{Forb}})$-VCS and a $(\Gamma''_{\text{Qual}}, \Gamma''_{\text{Forb}})$-VCS with basis matrices S'_0, S'_1 and S''_0, S''_1 respectively. We construct the VCS for the access structure $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}) = (\Gamma'_{\text{Qual}} \cup \Gamma''_{\text{Qual}}, \Gamma'_{\text{Forb}} \cap \Gamma''_{\text{Forb}})$ as follows.

We create matrices $\hat{S}'_0$, $\hat{S}'_1$, $\hat{S}''_0$, $\hat{S}''_1$ from S'_0, S'_1, S''_0, S''_1 respectively. We will show how to construct $\hat{S}'_0$. For $1 < i < n$, the i^{th} row of $\hat{S}'_0$ has all zero entries if participant i is not an essential participant, otherwise it is the same as the row of S'_0 corresponding to participant i. We construct $\hat{S}'_1$, $\hat{S}''_0$, $\hat{S}''_1$ similarly. Finally, we have $S_0 = \hat{S}'_0 \circ \hat{S}''_0$ and $S_1 = \hat{S}'_1 \circ \hat{S}''_1$, where $\circ$ is the concatenation of matrices.

It is important to note that this construction can only be used if the smaller access structures are realized using basis matrices.

A Starting Matrices Threshold Construction

Definition 2.4 A *starting matrix* $SM(n, l, k)$ is an $n \times l$ matrix whose entries are elements of a ground set $\{a_1, \ldots, a_k\}$ with the property that for any subset of k rows, there exists at least one column such that the entries in the k given rows are all distinct.

We use a starting matrix $SM(n, l, k)$ and an optimal (k, k)-VCS to construct $n \times (l \cdot 2^{k-1})$ basis matrices S_0 and S_1 for a (k, n)-threshold access structure by replacing the symbols $\{a_1, \ldots, a_k\}$ with the corresponding rows of the (k, k)-VCS.

2.2.3 Theory

Atienese, Blundo, De Santis, and Stinson [1] give optimal values for the pixel expansion for all access structures on four participants. In order to do this, they prove certain results regarding the structure of a VCS. Most of these results fall into one of two categories: unavoidable patterns and graph-based access structures.

We will first begin with some miscellaneous results on isolated participants and non-connected graphs.

Isolated Participants and Non-Connected Access Structures

First, Atienese, Blundo, De Santis, and Stinson [1] show that we need only consider access structures where $|X| \geq 2$ for all $X \in \Gamma_{\text{Qual}}$, that is, access structures with no isolated participants. To prove this, let $\mathcal{P}' = \mathcal{P} \setminus \{x\}$ and consider the induced access structure $(\Gamma'_{\text{Qual}}, \Gamma'_{\text{Forb}}) = (\Gamma_{\text{Qual}}[\mathcal{P}'], \Gamma_{\text{Forb}}[\mathcal{P}'])$. We can construct a VCS for $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ from a VCS for $(\Gamma'_{\text{Qual}}, \Gamma'_{\text{Forb}})$ as follows: for each matrix $M \in C'_0$, adjoin a row corresponding to x consisting of zeros. For each matrix $M \in C_1$, adjoin a row corresponding to x consisting of ones. Clearly Properties 1 and 2 of Definition 2.2 are satisfied, and the resulting sets of matrices constitute a VCS. In addition, if there are multiple isolated participants, this construction can be applied for each isolated participant.

Atienese, Blundo, De Santis, and Stinson [1] also show how to construct a VCS for an access structure with a participant x such that $\{x\} \cup X \in \Gamma_{\text{Qual}}$ for all $X \subseteq \mathcal{P} \setminus \{x\}$. In other words, x and any other group of participants are qualified. Let $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ be an access structure on a set of participants $\mathcal{P}$ where $x \notin \mathcal{P}$, and let $\Gamma'_{\text{Qual}} = \Gamma_{\text{Qual}} \cup \{X \cup \{x\} : X \subseteq \mathcal{P}\}$. Given collections of matrices C_0, C_1 representing a VCS with pixel expansion m on $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$, they show how to construct collections of matrices C'_0, C'_1 representing a VCS for $(\Gamma'_{\text{Qual}}, \Gamma_{\text{Forb}})$. For each $M \in C_0$, adjoin a new row corresponding to participant x consisting of zeros, and a column of zeros. For each $M \in C_1$ adjoin a row corresponding to participant x consisting of ones, and a column consisting of zeros, except that the entry in row

x, column $m+1$ is equal to one. Clearly Properties 1 and 2 of Definition 2.2 are satisfied, so the new collections constitute a VCS. This construction can be applied repeatedly if there is more than one such x.

Given an access structure $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ on a set of participants $\mathcal{P}$, we say that it is *connected* if it is not possible to partition $\mathcal{P}$ into $\mathcal{P}'$ and $\mathcal{P}''$ such that $\Gamma_{\text{Qual}} \subseteq 2^{\mathcal{P}'} \cup 2^{\mathcal{P}''}$. If such a partitioning can be found, we say the access structure is *non-connected.* We define the sum of two access structures $(\Gamma'_{\text{Qual}}, \Gamma'_{\text{Forb}})$ on $\mathcal{P}'$ and $(\Gamma''_{\text{Qual}}, \Gamma''_{\text{Forb}})$ on $\mathcal{P}''$ to be $\mathcal{P} = \mathcal{P}' \cup \mathcal{P}''$ with $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ such that $\Gamma_{\text{Qual}} = \Gamma'_{\text{Qual}} \cup \Gamma''_{\text{Qual}}$ and $\Gamma_{\text{Forb}} = \{X \cup Y : X \in \Gamma'_{\text{Forb}}, Y \in \Gamma''_{\text{Forb}}\}$. Atienese, Blundo, De Santis, and Stinson [1] prove the following theorem.

Theorem 2.1 *Let* $(\Gamma'_{\text{Qual}}, \Gamma'_{\text{Forb}})$ *and* $(\Gamma''_{\text{Qual}}, \Gamma''_{\text{Forb}})$ *be access structures on disjoint sets of participants* $\mathcal{P}'$ *and* $\mathcal{P}''$ *respectively, and let* $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ *be their sum. If there exist a* $(\Gamma'_{\text{Qual}}, \Gamma'_{\text{Forb}}, m')$*-VCS and* $(\Gamma''_{\text{Qual}}, \Gamma''_{\text{Forb}}.m'')$*-VCS, then there exists a* $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, m)$*-VCS where* $m = \max\{m', m''\}$.

Thus, we do not need to consider non-connected access structures, since their minimum pixel expansion can be determined from their connected parts.

Unavoidable Patterns

Unavoidable patterns are submatrices which must be present in the matrices which make up each collection. These submatrices are defined by the access structures. We denote by $M[X]$ the matrix M restricted to the rows corresponding to X, where $M \in C_0 \cup C_1$ and $X \subseteq \mathcal{P}$. Atienese, Blundo, De Santis, and Stinson [1] proved several results, which we will state here without proof. In all these results, $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ is an access structure on a set of participants $\mathcal{P}$.

Lemma 2.2 *Given $X, Y \subseteq \mathcal{P}$ such that $X \cap Y = \emptyset$ and $X \in \Gamma_{\text{Forb}}$, if there exists $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, m)$-VCS then any matrix $M \in C_1$ has the property that*

$$w(M[X \cup Y]) - w(M[X]) \geq \alpha(m) \cdot m.$$

We apply this theorem by choosing some $X \in \Gamma_{\text{Forb}}$ and $i \in \mathcal{P}$ such that $X \cup \{i\} \in \Gamma_{\text{Qual}}$. We get that

$$w(M[X \cup \{i\}]) - w(M[X]) \geq \alpha(m) \cdot m.$$

Therefore there must be $\alpha(m) \cdot m$ columns with a 1 in row i and 0 in the rows of X.

The following corollaries are immediate.

Corollary 2.3 *Given a strongly essential participant i such that $\{i\} \in \Gamma_{\text{Forb}}$, if there exists a $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, m)$-VCS then for any $M \in C_0 \cup C_1$ the inequality $w(M[\{i\}]) \geq \alpha(m) \cdot m$ holds.*

Corollary 2.4 *Given $X \in \Gamma_{\text{Qual}}$ such that $X \setminus \{i\} \in \Gamma_{\text{Forb}}$ for all $i \in X$, then in any $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, m)$-VCS, we have $t_X \geq |X| \cdot \alpha(m) \cdot m$.*

The first corollary tells us that for any strongly essential participant, there must be at least $\alpha(m) \cdot m$ ones in the row corresponding to that participant for any matrix in either collection. The second corollary tells us that the threshold value t_X must be greater than the number of participants in X multiplied by $\alpha(m) \cdot m$.

Finally, Atienese, Blundo, De Santis, and Stinson [1] give a result showing that for any qualified set of participants X and any matrix in C_0, $M[X]$ must contain at least $\alpha(m) \cdot m$ columns consisting of all zeros. We quote their result here for convenience.

Lemma 2.5 *Suppose $X \in \Gamma_{\text{Qual}}$. Then, in any $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, m)$-VCS for any $M \in C_0$, the matrix $M[X]$ has at least $\alpha(m) \cdot m$ columns with entries all equal to zero.*

Atienese, Blundo, De Santis, and Stinson [1] use these unavoidable patterns to prove results for complete bipartite graphs and $(3,3)$-threshold access structures. We quote their theorems here.

Theorem 2.6 *Let $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ be a strong access structure on the set of participants $\mathcal{P}$ containing no isolated participants. If there exists a $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, 2)$-VCS, then the basis Γ_0 is the edge-set of a complete bipartite graph.*

Theorem 2.7 *Let $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ be the access structure of a $(3,3)$-threshold VCS on the set of participants $\mathcal{P} = \{1,2,3\}$. In any $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, 4)$-VCS all matrices have a unique form up to a column permutation. That is, any matrix $M \in C_1$ and any matrix $M' \in C_0$ is equal, up to a column permutation, (respectively) to*

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \qquad M' = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Blundo, De Santis, and Stinson [3] later proved a more general version of this result stating that any (k,k)-threshold VCS with a specified pixel expansion must have basis matrices of a specified form. We quote their result for convenience. An *even column* refers to a column with an even number of ones, and an *odd column* refers to a column with an odd number of ones.

Theorem 2.8 *Let S_0 and S_1 be two $n \times m$ matrices such that the same column does not appear in both. Then the matrices S_0 and S_1 are basis matrices of a (k,k)-threshold VCS with pixel expansion m and relative difference $\alpha(m) = h/2^{k-1}$ if and only if all the even columns appear in S_0 with multiplicity $h = m/2^{k-1}$ and all the odd columns appear in S_1 with the same multiplicity h. Consequently, $h \geq \alpha(m) \cdot m$, $\alpha(m) \leq 1/2^{k-1}$, and $m \geq 2^{k-1}$.*

2.2.4 Threshold schemes

Atienese, Blundo, De Santis, and Stinson [1] show that for (k,n)-threshold VCS, each of the matrices in C_1 represent a $(k-1)$-cover-free family. A $(k-1)$-*cover-free family* consists of a ground set of elements G and family of sets $\mathcal{A} = \{A_1, \ldots, A_n\}$ such that the union of any $k-1$ of them does not cover any of the remaining sets, that is, $A_{j_1} \not\subseteq A_{j_2} \cup \ldots \cup A_{j_k}$ for any distinct $j_1, \ldots, j_k \in \{1, \ldots, n\}$. Thus we have the following result for the minimum pixel expansion of a (k,n)-threshold VCS.

Theorem 2.9 *The minimum pixel expansion for a (k,n)-threshold VCS is $m^* \geq \psi(n,k)$, where $\psi(n,k)$ is the size of the smallest ground set G for which a $(k-1)$-cover-free family exists.*

They also give a result on the size of such a cover-free family, leading to the following corollary.

Corollary 2.10 *For any (k,n)-threshold VCS with pixel expansion we have*

$$\binom{n}{k-1} \leq \binom{m}{\lfloor \frac{m}{2} \rfloor}$$

and $m = \Omega(k \log n)$.

2.2.5 Graph Access Structures

Atienese, Blundo, De Santis, and Stinson [1] proved several results for access structures based on graphs. The most significant is their theorem giving a value for the minimum pixel expansion for access structures based on complete multipartite graphs. They begin by finding the value of the minimum pixel expansion for complete graphs. Next, they use this result along with Lemma 4.8 to give a value for the minimum pixel expansion for graphs by using the maximum size clique. Finally, they use these theorems to prove the minimum pixel expansion for complete multipartite graphs and give a construction.

We start with proof of an upper bound for access structures based on K_n, which offers a construction based on Sperner families. A Sperner family consists of a ground set G and a set $\mathcal{SF} = \{A_1, A_2, \ldots, A_n\}$ of subsets of G such that $A_i \nsubseteq A_j$ for $i \neq j$.

Theorem 2.11 *Given a Sperner family $\mathcal{A} = \{A_1, \ldots, A_n\}$ on a ground set $G = \{g_1, \ldots, g_m\}$, we have that $m^*(K_n) \leq m$.*

We can construct the basis matrices from the Sperner family as follows. For $1 \leq i \leq n$ and $1 \leq j \leq m$, define

$$S_0(i,j) = \begin{cases} 1 & \text{if } 1 \leq j \leq |B_i|; \\ 0 & \text{if } |B_i| + 1 \leq j \leq m. \end{cases}$$

$$S_1(i,j) = \begin{cases} 1 & \text{if } g_j \in B_i; \\ 0 & \text{if } g_j \notin B_i. \end{cases}$$

Atienese, Blundo, De Santis, and Stinson [1] then apply a well-known result about Sperner families to obtain the following theorem.

Theorem 2.12 *The minimum pixel expansion for an access structure represented by a complete graph K_n is the smallest value m such that $n \leq \binom{m}{\lfloor \frac{m}{2} \rfloor}$.*

Let $\omega(G)$ represent the maximum size clique in a graph G. Recall that a clique is a complete subgraph of G. The following holds.

Theorem 2.13 *For any graph G, there exists a $(\Gamma(G), m)$-VCS only if $\omega(G) \leq \binom{m}{\lfloor \frac{m}{2} \rfloor}$.*

Finally, we give the minimum pixel expansion for access structures based on complete multipartite graphs. We also give the construction that is used to prove the result.

Theorem 2.14 *There exists a $\Gamma(K_{a_1,\ldots,a_n}, m)$-VCS if and only if $n \leq \binom{m}{\lfloor \frac{m}{2} \rfloor}$.*

Given basis matrices S_0, S_1 representing a VCS for the access structure based on the graph K_n, we construct $\hat{S}_0, \hat{S}_1$ by replicating row q of S_0, S_1 a_q times.

2.3 Grey Level VCS

2.3.1 The model

Blundo, De Santis, and Naor [2] extend the VCS model for general access structures to accommodate a specified number of grey levels, g. This definition for GVCS is taken nearly verbatim from their paper.

Definition 2.5 Let $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ be an access structure on n participants and let $g \geq 2$ be an integer. The g collections of $n \times m$ Boolean matrices $C_0, \ldots, C_{g-1}$ form a visual cryptography scheme with g grey levels and pixel expansion m if there exist values $\alpha_0, \ldots, \alpha_{g-2}$ and sets $\{X, t_{i,X}\}_{X \in \Gamma_{\text{Qual}}}$ for $0 \leq i \leq g-2$ satisfying:

1. Any $X = \{j_1, \ldots, j_p\} \in \Gamma_{\text{Qual}}$ can recover the shared image by combining their shares. Formally, for $i = 0, \ldots, g-2$ for any $M \in C_i$, the *OR* V of rows $j_1, \ldots, j_p$ satisfies $w(V) \leq t_{i,X} - \alpha_i \cdot m$; whereas for any $M \in C_{i+1}$ we have that $w(V) \geq t_{i,X}$.

2. Any $X = \{j_1, \ldots, j_p\} \in \Gamma_{\text{Forb}}$ has no information on the shared image. Formally, the g collections of $p \times m$ matrices D_i, $0 \leq i \leq g-1$, obtained by restricting each $n \times m$ matrix in C_i to rows $j_1, \ldots, j_p$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

Note that the set of thresholds $\{t_X\}$ and relative difference α must now vary according to the grey level. We therefore have thresholds $\{t_{i,X}\}$ and relative differences $\{\alpha_i\}$ where $0 \leq i \leq g-2$.

The first property ensures that the participants will be able to distinguish the g grey levels. The quantity $\alpha_i \cdot m$ is known as the contrast for grey level i. We require that $\alpha_i \cdot m \geq 1$, $0 \leq i \leq g-2$ to ensure that the participants can distinguish all the grey levels.

The second property ensures the security of the scheme. Even by inspecting all their shares, a set of forbidden participants will not be able to gain any information on the secret image.

Once again, we rewrite the definition in terms of basis matrices, taken nearly verbatim from Blundo, De Santis, and Naor [2].

Definition 2.6 Let $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ be an access structure on n participants and let $g \geq 2$ be an integer. The g Boolean matrices $G_0, \ldots, G_{g-1}$ are a visual cryptography scheme with g grey levels and pixel expansion m if there exist values $\alpha_0, \ldots, \alpha_{g-2}$ and sets $\{X, t_{i,X}\}_{X \in \Gamma_{\text{Qual}}}$ for $0 \leq i \leq g-2$ satisfying:

1. If $X = \{j_1, \ldots, j_p\} \in \Gamma_{\text{Qual}}$ then for $0 \leq i \leq g-2$, the *OR* V of rows $j_1, \ldots, j_p$ of G_i satisfies $w(V) \leq t_{i,X} - \alpha_i \cdot m$; whereas for G_{i+1} we have that $w(V) \geq t_{i,X}$.

2. If $X = \{j_1, \ldots, j_p\} \in \Gamma_{\text{Forb}}$ then the g $p \times m$ matrices $G_0, \ldots, G_{g-1}$ obtained by restricting them to rows $j_1, \ldots, j_p$ are equal up to a column permutation.

The collections of matrices C_i in Definition 2.5 may be obtained by generating all permutations of the basis matrices G_i.

Blundo, De Santis, and Naor [2] also prove the following result giving the optimal pixel expansion for (k, k) threshold access structures.

Lemma 2.15 *In any (k, k, m, g)-GVCS with relative differences $\alpha_0, \ldots, \alpha_{g-2}$, we have*

$$\min\{\alpha_0, \ldots, \alpha_{g-2}\} \leq 1/(g-1)2^{k-1}$$

and

$$m \geq (g-1)2^{k-1}.$$

2.3.2 A construction

Given basis matrices for a $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ VCS with relative difference α^* and pixel expansion $\bar{m}$, Blundo et al. [2] show how to construct a GVCS with relative differences $\alpha_0, \ldots, \alpha_{g-2}$ such that $\sum_{i=0}^{g-2} \alpha_i \leq \alpha^*$. Let $\alpha_i = a_i/b_i$, $0 \leq i \leq g-2$ and $\alpha^* = a/b$ such that a_i, b_i, a, b are positive integers. Compute

$$m = \text{lcm}\{b_0, \ldots, b_{g-2}\} \cdot a \cdot \bar{m}, \tag{2.1}$$

$$r_i = \frac{a_i \cdot b \cdot m}{b_i \cdot a \cdot \bar{m}}, \text{ and} \tag{2.2}$$

$$d = m - \sum_{i=0}^{g-2} r_i \cdot \bar{m}. \tag{2.3}$$

We need to show that $d = m - \sum_{i=0}^{g-2} r_i \cdot \bar{m} \geq 0$. To achieve this, note that (2.2) can be rewritten as

$$r_i = \frac{\alpha_i \cdot m}{\alpha^* \cdot \bar{m}}. \tag{2.4}$$

We now have

$$\begin{aligned}
d \geq 0 &\Leftrightarrow m - \sum_{i=0}^{g-2} r_i \cdot \bar{m} \geq 0 \\
&\Leftrightarrow m - \sum_{i=0}^{g-2} \frac{\alpha_i \cdot m}{\alpha^* \cdot \bar{m}} \cdot \bar{m} \geq 0 \\
&\Leftrightarrow m - \sum_{i=0}^{g-2} \frac{\alpha_i \cdot m}{\alpha^*} \geq 0 \\
&\Leftrightarrow m - m \cdot \sum_{i=0}^{g-2} \frac{\alpha_i}{\alpha^*} \geq 0 \\
&\Leftrightarrow m \left(1 - \sum_{i=0}^{g-2} \frac{\alpha_i}{\alpha^*} \right) \geq 0 \\
&\Leftrightarrow 1 - \sum_{i=0}^{g-2} \frac{\alpha_i}{\alpha^*} \geq 0 \\
&\Leftrightarrow \frac{1}{\alpha^*} \sum_{i=0}^{g-2} \alpha_i \leq 1 \\
&\Leftrightarrow \sum_{i=0}^{g-2} \alpha_i \leq \alpha^*.
\end{aligned}$$

Since $\sum_{i=0}^{g-2} \alpha_i \leq \alpha^*$ by hypothesis, we have $d \geq 0$.

Let D be the zero matrix of size $n \times d$. For $0 \leq i \leq g-1$, define

$$G_i = \underbrace{S_0 \circ \ldots \circ S_0}_{\sum_{j=i}^{g-2} r_j} \circ \underbrace{S_1 \circ \ldots \circ S_1}_{\sum_{j=0}^{i-1} r_j} \circ D.$$

Finally, we let $t_{i-1,X} = w(G_i[X])$. For the remaining details of the proof, see [2].

Chapter 3

GVCS Constructions

3.1 An optimal (t, t) threshold construction

The (t, t)-GVCS construction that is obtained from using the technique proposed by Blundo, De Santis, and Naor [2] has a less than optimal pixel expansion. They have shown that the optimal pixel expansion for a (t, t)-GVCS is $m \geq (g - 1)2^{t-1}$. We can use the optimal (t, t)-VCS from Naor and Shamir [6] to create a GVCS with pixel expansion $m = (g - 1)2^{t-1}$. Since we will be using a (t, t)-GVCS construction in more general constructions, it is important to have a "base" construction with an optimal pixel expansion. Assuming that the total number of grey levels is g, for each grey level k we can assume that a pixel with grey level k is a union of k black subpixels and $g - k - 1$ white subpixels. We begin with an optimal $(t, t)-$VCS, which has basis matrices S_0, S_1 and pixel expansion $m = 2^{t-1}$. The basis matrices

G_i are simply the concatenation of $g - i - 1$ copies of S_0 and i copies of S_1.

$$G_i = \underbrace{S_0 \circ \ldots \circ S_0}_{g-i-1} \circ \underbrace{S_1 \circ \ldots \circ S_1}_{i}.$$

The set of threshold values $\{t_{i,X}\}$ are $t_{i,X} = m-g+i+2$ and the relative differences are $\alpha_i = 1/m$. Since we are concatenating $g - 1$ matrices, we have pixel expansion $m = (g - 1)2^{t-1}$, which is optimal.

Example 3.1 We will now show how to construct a $(3, 3)$-GVCS with 4 grey levels. In order to generate the basis matrices for a $(3, 3)$-GVCS with this construction, we need the basis matrices for an optimal $(3, 3)$-VCS. Using the construction provided by Naor and Shamir [6], we get:

$$S_0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \quad S_1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

Using these in our construction, we get:

$$G_0 = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix};$$

$$G_1 = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix};$$

$$G_2 = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix};$$

$$G_3 = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

We have $m = 12$, $t_0 = 10$, $t_1 = 11$, $t_2 = 12$, and $\alpha_0 = \alpha_1 = \alpha_2 = 1/12$.

Theorem 3.1 *There exists a (k, k, g, m)-GVCS with $m = 2^{k-1}$, set of threshold values $t_{i,X} = m - g + i + 2$ and relative difference $\alpha_i = 1/m$.*

Proof. Note that in G_{g-1} there are no columns with all zero entries. In G_{g-2} there is 1 such column, and in G_0 there are $g-1$ such columns. In general, for matrix G_i, there are $g - i - 1$ columns with all zero entries. Consequently, when we compute the *OR V* of all k rows on matrix G_i, we get

$$w(V) = m - (g - i - 1) = m - g + i + 1.$$

Let $t_{i,X} = m - g + i + 2$. We have that

$$t_{i,X} - \alpha_i(m) \cdot m = (m - g + i + 2) - (1/m \cdot m) = m - g + i + 1.$$

Therefore we have $w(V) \leq t_{i,X} - \alpha_i(m) \cdot m$ as required. If we compute the *OR* V of all k rows on matrix G_{i+1}, we have

$$w(V) = m - (g - (i+1) - 1) = m - g + i + 2.$$

Therefore $w(V) \geq t_{i,X}$, and Property 1 is satisfied.

To prove Property 2, we consider each adjacent pair of basis matrices G_i, G_{i+1} for $1 \leq i \leq g-2$. Let $X \subset \mathcal{P}$, where $|X| < t$. Then G_i contains $g-i-1$ copies of S_0 and i copies of S_1, and G_{i+1} contains $g-i-2$ copies of S_0 and $i+1$ copies of S_1. Since each contains $g-i-2$ copies of S_0 and i copies of S_1, these columns are clearly equal for any choice of participants X. The remaining columns of G_i are equal to S_0 and the remaining columns of G_{i+1} are equal to S_1. From Naor and Shamir [6], and Atienese, Blundo, De Santis, and Stinson [1] we have that $S_0[X] = S_1[X]$ up to a column permutation, and therefore $G_i[X] = G_{i+1}[X]$ up to a column permutation. Since this is true for any $0 \leq i \leq g-2$, we have that all $G_i[X]$ equal up to a column permutation for $0 \leq i \leq g-1$. Thus we have proven Property 2, and this construction is a valid GVCS. ■

3.2 A cumulative arrays construction

Using the (t,t)-GVCS construction, we can derive a construction for a general access structure $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ based on the cumulative arrays construction for VCS given by Atienese, Blundo, De Santis, and Stinson [1].

To construct the cumulative array CA, we use the set of maximal forbidden sets

$Z_M = \{F_0, \ldots, F_{t-1}\}$. Here CA is a $|\mathcal{P}| \times t$ boolean matrix where $CA[i,j] = 1$ if and only if $i \notin F_j$.

Let $\hat{G}_0, \ldots, \hat{G}_{g-1}$ be the basis matrices of a (t,t) threshold GVCS with g grey levels. We construct the basis matrices $G_0, \ldots, G_{g-1}$ as follows. For any fixed i, let $j_{i,1}, \ldots, j_{i,g_i}$ be the integers j such that $CA[i,j] = 1$. For each $0 \leq k \leq g-1$, the i^{th} row of G_k is the OR of rows $j_{i,1}, \ldots, j_{i,g_i}$ of $\hat{G}_k$. This construction yields a pixel expansion of $(g-1)2^{t-1}$, where t is the size of the set of maximal forbidden sets of $\mathcal{P}$, the relative difference is $\alpha_i = 1/m$, and the threshold values are the same as those of the $(t,t)-$GVCS used in the construction.

Example 3.2

Let $\mathcal{P} = \{P_1, P_2, P_3, P_4, P_5\}$. Let $\Gamma_0 = \{\{P_1, P_5\}, \{P_2, P_4\}, \{P_3, P_4, P_5\}\}$ be the set of minimal qualified subsets. The set of maximal forbidden subsets is $Z_M = \{\{P_1, P_2, P_3\}, \{\{P_1, P_4\}, \{P_2, P_5\}\}$. Since we have $|Z_M| = 3$, we will use the basis matrices for the $(3,3)$ threshold GVCS already computed in Example 3.1. We will call these basis matrices $\hat{G}_0, \hat{G}_1, \hat{G}_2, \hat{G}_3$. We compute the cumulative array as given to obtain:

$$CA = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

From this, we see that the first row of G_i is the third row of $\hat{G}_i$, the second row of G_i is the second row of $\hat{G}_i$, the third row of $\hat{G}_i$ is the OR of rows 2 and 3 of $\hat{G}_i$, and so on. We therefore have the following basis matrices realizing the given access structure.

$$G_0 = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix};$$

$$G_1 = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix};$$

$$G_2 = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix};$$

$$G_3 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Theorem 3.2 *Given a strong access structure* $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ *such that* Z_M *is the family of maximal forbidden subsets in* Γ_{Forb} *(where* $|Z_M| = t$*), there exists a* $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, m, g)$*-GVCS with* $m = (g-1)2^{t-1}$, $\{t_{i,X}\} = \{t'_{i,X}\}$*, and* $\alpha_i = \frac{1}{m}$*, where* $\{t'_{i,X}\}$ *are the threshold values of an optimal* (t,t)*-GVCS.*

Proof. Each adjacent pair of matrices can be considered as a regular VCS. To prove that the previous construction works, we show that each grey level i, $1 \leq i \leq g-2$, is distinguishable from the grey level immediately before and after.

Consider the case where $i = 1$. We construct G_0, G_1 from $\hat{G}_0$, $\hat{G}_1$ using the previous construction, with set of thresholds $\{t_{0,X}\}$ and relative difference α_0. Next we construct G_1, G_2 from $\hat{G}_1$, $\hat{G}_2$ as before, with thresholds $\{t_{1,X}\}$ and relative difference α_1. Note that G_1 will be the same as before by the construction technique. Additionally, if X is a qualified set, then we have $G_1 \geq t_{0,X}$ from the first and $G_1 \leq t_{1,X} - \alpha_1 m$. This means that grey level 1 will be distinguishable from both levels 0 and 2. If X is not a qualified set, then $G_0[X] = G_1[X]$ and $G_1[X] = G_2[X]$, so they are all equal up to a column permutation.

We continue similarly until $i = g-2$. Clearly each grey level $1 \leq i \leq g-2$ is distinguishable from grey levels $i-1$ and $i+1$ if X is a valid set, and all $G_i[X]$ are equal up to a column permutation if X is a forbidden set. Therefore $G_0, \ldots, G_{g-1}$ are the basis matrices of a GVCS realizing the general access structure $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ with set of thresholds $\{t_{i,X}\}$ and relative differences α_i where $0 \leq i \leq g-1$. ■

3.3 A decomposition construction

Another method of construction for general access structures is the decomposition construction, which uses smaller access structures as building blocks for larger ones.

Let $(\Gamma'_{\text{Qual}}, \Gamma'_{\text{Forb}})$ and $(\Gamma''_{\text{Qual}}, \Gamma''_{\text{Forb}})$ be two access structures on a set of n participants $\mathcal{P}$. If a participant $i \in \mathcal{P}$ is non-essential for $(\Gamma'_{\text{Qual}}, \Gamma'_{\text{Forb}})$, we assume that $i \in \Gamma'_{\text{Forb}}$ and that i does not receive nothing as a share. Similarly for $(\Gamma''_{\text{Qual}}, \Gamma''_{\text{Forb}})$.

Suppose there exist a $(\Gamma'_{\text{Qual}}, \Gamma'_{\text{Forb}})-$GVCS and a $(\Gamma''_{\text{Qual}}, \Gamma''_{\text{Forb}})-$GVCS with basis matrices $G'_0, \ldots, G'_{g-1}$ and $G''_0, \ldots, G''_{g-1}$ respectively. We will show how to construct a GVCS for the access structure $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}) = (\Gamma'_{\text{Qual}} \cup \Gamma''_{\text{Qual}}, \Gamma'_{\text{Forb}} \cap \Gamma''_{\text{Forb}})$.

From the matrices $G'_0, \ldots, G'_{g-1}$ and $G''_0, \ldots, G''_{g-1}$, we will construct new matrices $\hat{G}'_0, \ldots, \hat{G}'_{g-1}$ and $\hat{G}''_0, \ldots, \hat{G}''_{g-1}$, each consisting of n rows, as follows. For $1 \leq i \leq n$, the i^{th} row of $\hat{G}'_j$ is all zero if i is not an essential participant of $(\Gamma'_{\text{Qual}}, \Gamma'_{\text{Forb}})$, otherwise it is the row of G'_j corresponding to participant i. Similarly for $\hat{G}''_j$. Finally, the basis matrices $G_0, \ldots, G_{g-1}$ will be realized by concatenating the corresponding matrices, that is $G_j = \hat{G}'_j \circ \hat{G}''_j$.

Theorem 3.3 *Given a $(\Gamma'_{\text{Qual}}, \Gamma'_{\text{Forb}}, g, m')$-GVCS with basis matrices $G'_0, \ldots, G'_{g-1}$ and a $(\Gamma''_{\text{Qual}}, \Gamma''_{\text{Forb}}, g, m'')$-GVCS with basis matrices $G''_0, \ldots, G''_{g-1}$, there exists a*

$(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, g, m)$*-GVCS with basis matrices* $G_0, \ldots, G_{g-1}$ *where* $\Gamma_{\text{Qual}} = \Gamma'_{\text{Qual}} \cup \Gamma''_{\text{Qual}}$*,* $\Gamma_{\text{Forb}} = \Gamma'_{\text{Forb}} \cap \Gamma''_{\text{Forb}}$*, and* $m = m' + m''$*.*

Proof. We will show that the decomposition construction works by giving values for m and $\alpha_i(m)$ and proving that the construction works for four cases:

1. X is in Γ'_{Qual} and Γ''_{Qual};

2. X is in Γ'_{Qual} but not in Γ''_{Qual};

3. X is in Γ''_{Qual} but not in Γ'_{Qual};

4. X is in Γ'_{Forb} and Γ''_{Forb}.

In the first three cases, X is in Γ_{Qual}, and we show that for any i, $G_i[X] \leq t_{i,X} - \alpha_i(m) \cdot m$ and $G_{i+1}[X] \geq t_{i,X}$. In the last case, X is in Γ_{Forb}, and we show that $G_0[X] = G_1[X] = \ldots = G_{g-1}[X]$.

Let m' and m'' be the pixel expansions for the basis matrices corresponding to $(\Gamma'_{\text{Qual}}, \Gamma'_{\text{Forb}})$ and $(\Gamma''_{\text{Qual}}, \Gamma''_{\text{Forb}})$. Let $\{X, t'_{i,X}\}_{\substack{X \in \Gamma'_{\text{Qual}} \\ i \in \{0,\ldots,g-1\}}}$ and $\{X, t''_{i,X}\}_{\substack{X \in \Gamma''_{\text{Qual}} \\ i \in \{0,\ldots,g-1\}}}$ be the set of thresholds, and $\alpha'_i(m')$ and $\alpha''_i(m'')$ be the relative differences. Define $m = m' + m''$ and

$$\alpha_i(m) = \frac{\min\{\alpha'_i(m') \cdot m', \alpha''_i(m'') \cdot m''\}}{m}.$$

Let X be a set of participants.

Case 1: $X \in \Gamma'_{\text{Qual}} \cap \Gamma''_{\text{Qual}}$. Let $t_{i,X} = t'_{i,X} + t''_{i,X}$.

$$\begin{aligned}
w(G_i[X]) &= w(\hat{G}'_i[X] \circ \hat{G}''_i[X]) \\
&= w(\hat{G}'_i[X]) + w(\hat{G}''_i[X]) \\
&= w(G'_i[X]) + w(G''_i[X]) \\
&\leq (t'_{i,X} - \alpha'_i(m') \cdot m') + (t''_{i,X} - \alpha''_i(m'') \cdot m'') \\
&\leq t'_{i,X} + t''_{i,X} - (\alpha'_i(m') \cdot m' + \alpha''_i(m'') \cdot m'') \\
&\leq t_{i,X} - \alpha_i(m) \cdot m
\end{aligned}$$

since $\alpha'_i(m') \cdot m' + \alpha''_i(m'') \cdot m'' \geq \min\{\alpha'_i(m') \cdot m', \alpha''_i(m'') \cdot m''\} = \alpha_i(m) \cdot m$. Also

$$\begin{aligned}
w(G_{i+1}[X]) &= w(\hat{G}'_{i+1}[X] \circ \hat{G}''_{i+1}[X]) \\
&= w(\hat{G}'_{i+1}[X]) + w(\hat{G}''_{i+1}[X]) \\
&= w(G'_{i+1}[X]) + w(G''_{i+1}[X]) \\
&\geq t'_{i,X} + t''_{i,X} \\
&\geq t_{i,X}.
\end{aligned}$$

Case 2: $X \in \Gamma'_{\text{Qual}} \setminus \Gamma''_{\text{Qual}}$. Let $t_{i,X} = t'_{i,X} + w(\hat{G}_i[X])$.

$$\begin{aligned}
w(G_i[X]) &= w(\hat{G}'_i[X] \circ \hat{G}''_i[X]) \\
&= w(\hat{G}'_i[X]) + w(\hat{G}''_i[X]) \\
&= w(G'_i[X]) + w(G''_i[X]) \\
&\leq (t'_{i,X} - \alpha'_i(m') \cdot m') + w(G''_i[X]) \\
&\leq t'_{i,X} + w(G''_i[X]) - \alpha'_i(m') \cdot m' \\
&\leq t_{i,X} - \alpha_i(m) \cdot m
\end{aligned}$$

since $\alpha'_i(m') \cdot m' \geq \min\{\alpha'_i(m') \cdot m', \alpha''_i(m'') \cdot m''\} = \alpha_i(m) \cdot m$.

$$\begin{aligned}
w(G_{i+1}[X]) &= w(\hat{G}'_{i+1}[X] \circ \hat{G}''_{i+1}[X]) \\
&= w(\hat{G}'_{i+1}[X]) + w(\hat{G}''_{i+1}[X]) \\
&= w(G'_{i+1}[X]) + w(\hat{G}''_{i+1}[X]) \\
&\geq t'_{i,X} + w(\hat{G}''_{i+1}[X]) \\
&\geq t_{i,X}.
\end{aligned}$$

Case 3: $X \in \Gamma''_{\text{Qual}} \setminus \Gamma'_{\text{Qual}}$. Similar to case 2.

Case 4: $X \in \Gamma'_{\text{Forb}} \cap \Gamma''_{\text{Forb}}$. We have

$$\begin{aligned} G_i[X] &= \hat{G}_i[X]' \circ \hat{G}_i[X]'' \\ &= \hat{G}_{i+1}[X]' \circ \hat{G}_{i+1}[X]'' \\ &= G_{i+1}[X] \end{aligned}$$

up to a column permutation. ■

3.4 A (k, n) threshold construction

Atienese, Blundo, De Santis, and Stinson [1] use starting matrices to construct (k, n) threshold schemes using a (k, k) threshold scheme, for which we have an optimal construction. See Definition 2.4 for an explanation of starting matrices. We will use a similar technique to provide a construction for (k, n)-GVCS.

Given a matrix $SM(n, l, k)$, we can construct a (k, n) threshold GVCS as follows: the $n \times (l \cdot (g-1) \cdot 2^{k-1})$ basis matrices $G_0, \ldots, G_{g-1}$ are constructed by replacing the symbols $a_1, \ldots, a_k$ with the $1^{st}, \ldots, k^{th}$ rows of the corresponding basis matrix of the optimal (k, k)-GVCS, respectively.

Theorem 3.4 *Given a starting matrix $SM(n, l, k)$, there exist basis matrices for a (k, n, g, m)-threshold GVCS with pixel expansion $m = l \cdot (g-1) \cdot 2^{k-1}$.*

Proof. Let $G_0^k, \ldots, G_{g-1}^k$ be the basis matrices of an optimal (k, k)-GVCS and let $SM(n, l, k)$ be a starting matrix whose entries are elements of a ground set

$\{a_1, \ldots, a_k\}$. Let $G_0, \ldots, G_{g-1}$ be $n \times (l \cdot (g-1) \cdot 2^{k-1})$ matrices constructed by replacing the symbols $\{a_1, \ldots, a_k\}$ with the $1^{st}, \ldots, k^{th}$ rows of $G_0^k, \ldots, G_{g-1}^k$ respectively.

The basic block $B_{i,j}$ is the $n \times ((g-1) \cdot 2^{k-1})$ matrix obtained by expanding column j of the starting matrix using G_i^k.

Choose any adjacent pair of basic blocks $B_{i,j}, B_{i+1,j}$ (from adjacent matrices G_i, G_{i+1}). Fix any $d \geq k$ rows of these basic blocks. Either these rows comprise all the rows of G_i^k (G_{i+1}^k respectively) where any row can appear more than once, and thus their OR has weight $t_i - 1$ (t_i respectively); or they contain at most $k-1$ distinct rows and have the same weight in both basic blocks. We know that the first situation will be true for at least one j for any choice of $d \geq k$ rows, so we have Property 1.

To prove Property 2, we need to show that for any $X \subseteq \{1, \ldots, n\}$ with $|X| < k$, we have that $G_0[X] = \ldots = G_{g-1}[X]$ up to a column permutation. This is true since $B_{0,j} = \ldots = B_{g-1,j}$ up to a column permutation for all $1 \leq j \leq l$. ■

Note that in this construction, the thresholds will vary by choice of X.

Chapter 4

GVCS on Four Participants

In this chapter, we will develop the theories necessary to obtain values (or at least ranges of values) for the minimum pixel expansion for all strong, connected access structures with no isolated participants on four participants. We will also give some results for access structures which are not connected or which have isolated participants.

In the first section, we will begin with access structures that have isolated participants and access structures such that the graph representing them is not connected. In the next section, we will discuss *unavoidable patterns.* Unavoidable patterns are submatrices which must be present in the matrices which make up each collection. These submatrices are defined by the access structures.

In the next section, we will discuss access structures based on graphs. We will utilize the results in the prior section on unavoidable patterns to give values (or at least ranges of values) for the minimum pixel expansion for grey-level visual cryptography schemes for access structures based on graphs. The main result of the section is a value for the minimum pixel expansion for access structures based on complete multipartite graphs. Although not a graph-based access structure (except for the case $k = 2$), we will give a lower bound on the pixel expansion for (k, n) threshold access structures.

Finally, we will also show lower bounds on certain access structures which are not covered by any of the other results of this section. All results will be summarized in a table which shows the minimum pixel expansion for access structures when four grey levels are used.

4.1 General Theory

4.1.1 Isolated Participants and Non-Connected Graphs

This lemma shows how we can construct a GVCS for access structures with one isolated participant. This lemma can be applied iteratively for additional isolated participants.

Lemma 4.1 *Given an access structure* $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ *on* $\mathcal{P}$*and a participant* $x \notin \mathcal{P}$*, if a* $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, g, m)$*-GVCS exists, then there exists a* $(\Gamma_{\text{Qual}} \cup \{\{x\}\}, \Gamma_{\text{Forb}}, g, m)$*-GVCS.*

Proof. We construct the $(\Gamma_{\text{Qual}} \cup \{\{x\}\}, \Gamma_{\text{Forb}}, g, m)$-GVCS as follows. For any $M \in C_i$ where $1 \leq i \leq g - 1$, we add a new row corresponding to x, consisting of $\sum_{j=0}^{i-1} \alpha_j(m) \cdot m$ 1's and $m - \sum_{j=0}^{i-1} \alpha_j(m) \cdot m$ 0's. For any $M \in C_0$ we add a new row corresponding to x, consisting of 0's. We set $t_{i,\{x\}} = \sum_{j=0}^{i} \alpha_j(m) \cdot m$. Clearly this new construction satisfies Properties 1 and 2 of Definition 2.5 by its construction.■

The next lemma shows how to construct a GVCS for an access structure such that there exists a participant x such that x with any other participant in $\mathcal{P}$ is qualified. As in the above lemma, we must first have a GVCS for the access structure without participant x. As with the previous lemma, this result can be applied iteratively.

Lemma 4.2 *Given an access structure* $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ *on* $\mathcal{P}$ *and a participant* $x \notin \mathcal{P}$*, if a* $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, g, m)$*-GVCS exists, then there also exists a* $(\Gamma'_{\text{Qual}}, \Gamma_{\text{Forb}}, g, m+1)$*-GVCS where* $\Gamma'_{\text{Qual}} = \Gamma_{\text{Qual}} \cup \{X \cup \{x\} : X \subseteq \mathcal{P}\}$*.*

Proof. For any $M \in C_i$ where $1 \leq i \leq g-1$, we add a row corresponding to participant x consisting of $\sum_{j=0}^{i-1} \alpha_j(m) \cdot m$ 1s and $m - \sum_{j=0}^{i-1} \alpha_j(m) \cdot m$ 0s, and a column of 0s, except that the entry in row x, column $m+1$ is a 1. For any $M \in C_0$ we add a row corresponding to participant x consisting of 0s, and a column of 0s. We set the values $t_{i,X\cup\{x\}} = (\sum_{j=0}^{i-1} \alpha_j(m) \cdot m) + 1$. Clearly this construction satisfies Properties 1 and 2 of Definition 2.5. ■

The next lemma will be useful for proving a theorem on non-connected graphs. It allows us to concatenate any $n \times p$ matrix D to each matrix in the collections C_i. If the original GVCS represented by these collections had pixel expansion m, the resulting set of collections will be a GVCS on the same access structure with pixel expansion $m+p$.

Lemma 4.3 *Given a* $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, g, m)$*-GVCS with collections of matrices* C_i *and* D *any* $n \times p$ *boolean matrix, the collections of matrices* $C'_i = \{M \circ D : M \in C_i\}$ *form a* $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, g, m+p)$*-GVCS.*

Proof. Clearly Properties 1 and 2 of Definition 2.5 remain satisfied. We now have a set of thresholds $t'_{i,X} = t_{i,X} + w(D[X])$ and relative differences $\alpha'_i(m+p) = (\alpha_i(m) \cdot m)/(m+p)$. ■

We will now use this lemma to show a construction for access structures based on non-connected graphs given collections of matrices realizing a GVCS for the non-connected parts.

Theorem 4.4 *Let* $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ *be an access structure on a set of participants* $\mathcal{P}$ *such that the graph which represents it has two non-connected parts. Let* $\mathcal{P}'$ *and* $\mathcal{P}''$ *represent these parts, with* $\mathcal{P}' \cup \mathcal{P}'' = \mathcal{P}$*. Let* $(\Gamma'_{\text{Qual}}, \Gamma'_{\text{Forb}})$ *and* $(\Gamma''_{\text{Qual}}, \Gamma''_{\text{Forb}})$ *represent the corresponding access structures such that* $\Gamma_{\text{Qual}} = \Gamma'_{\text{Qual}} \cup \Gamma''_{\text{Qual}}$ *and* $\Gamma_{\text{Forb}} = \{X \cup Y : X \in \Gamma'_{\text{Forb}}, Y \in \Gamma''_{\text{Forb}}\}$*. Given a* $(\Gamma'_{\text{Qual}}, \Gamma'_{\text{Forb}}, g, m')$*-GVCS and a* $(\Gamma''_{\text{Qual}}, \Gamma''_{\text{Forb}}, g, m'')$*-GVCS, we can construct a* $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, g, m)$*-GVCS with* $m = \max(m', m'')$*.*

Proof. Let C'_i (C''_i respectively) denote the collections of matrices representing the GVCS for $(\Gamma'_{\text{Qual}}, \Gamma'_{\text{Forb}})$ $((\Gamma''_{\text{Qual}}, \Gamma''_{\text{Forb}}))$. Let $|C'_i| = r'$ and $|C''_i| = r''$. Without loss of generality assume $m' > m''$. Applying Lemma 4.3 we can construct a $(\Gamma''_{\text{Qual}}, \Gamma''_{\text{Forb}}, g, m')$-GVCS with collection of matrices C'''_i. We can now construct the matrices C_i as follows:

$$C_i = \{M : M[\mathcal{P}'] \in C'_i, M[\mathcal{P}''] \in C'''_i\}.$$

For any matrix in C'_i, we have r'' matrices in C_i. Thus $|C_i| = r' \cdot r''$.

It is easy to see that Property 1 holds. To verify Property 2, let $X \in \Gamma'_{\text{Forb}}$ ($X \in \Gamma''_{\text{Forb}}$ respectively) and $M \in \cup_{i=0}^{g-1} C'_i$ ($M \in \cup_{i=0}^{g-1} C'''_i$). Let η_X^i (μ_X^i) be the number of times the matrix $M[X]$ appears in the collection $\{A[X] : A \in C'_i\}$ ($\{A[X] : A \in C'''_i\}$). Property 2, applied to the original access structures, tells us that $\eta_X^0 = \cdots = \eta_X^{g-1}$ and $\mu_X^0 = \cdots = \mu_X^{g-1}$.

For any matrix $M \in \cup_{i=0}^{g-1} C_i$ we let γ_X^i denote the number of times the matrix $M[X]$ appears in $A[X] : A \in C_i$. We need to prove $\gamma_X^0 = \cdots = \gamma_X^{g-1}$ for any $X \in \Gamma_{\text{Forb}}$. If $X \subseteq \mathcal{P}'$ then the following equalities hold:

$$\eta_X^0 = \eta_X^1 = \cdots = \eta_X^{g-2} = \eta_X^{g-1}$$

$$\eta_X^0 r'' = \eta_X^1 r'' = \cdots = \eta_X^{g-2} r'' = \eta_X^{g-1} r''$$

$$\gamma_X^0 = \gamma_X^1 = \cdots = \gamma_X^{g-2} = \gamma_X^{g-1}$$

since $\gamma_X^i = \eta_X^i r''$, and similarly if $X \subseteq \mathcal{P}''$.

If $X = Y \cup Z$, $Y \in \Gamma'_{\text{Forb}}$ and $Z \in \Gamma''_{\text{Forb}}$ then

$$\eta_Y^0 \mu_Z^0 = \eta_Y^1 \mu_Z^1 = \cdots = \eta_Y^{g-2} \mu_Z^{g-2} = \eta_Y^{g-1} \mu_Z^{g-1}$$

$$\gamma_X^0 = \gamma_X^1 = \cdots = \gamma_X^{g-2} = \gamma_X^{g-1}$$

since $\gamma_X^i = \eta_Y^i \mu_Z^i$. ■

4.1.2 Unavoidable Patterns

We now examine the unavoidable patterns in the collections of matrices for grey level visual cryptography schemes. We will use these results later to help characterize the access structures on four participants. Throughout this section, we assume that $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ is an access structure on a set of participants $\mathcal{P}$.

Lemma 4.5 *Given $X, Y \subseteq \mathcal{P}$ such that $X \neq \emptyset$, $Y \neq \emptyset$, $X \cap Y = \emptyset$, $X \in \Gamma_{\text{Forb}}$, $X \cup Y \in \Gamma_{\text{Qual}}$, and any $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, g, m)$-GVCS, for any matrix $M \in C_i$, $1 \leq i \leq g-1$, we have*

$$w(M[X \cup Y]) - w(M[X]) \geq \sum_{j=0}^{i-1} \alpha_j(m) \cdot m.$$

Proof. Let $M \in C_i$. We know from Property 1 of Definition 2.5 that $w(M[X \cup Y]) \geq t_{i-1,X\cup Y}$. Property 2 tells us that there exists a matrix $M' \in C_0$ such that $M[X] = M'[X]$, since $X \in \Gamma_{\text{Forb}}$. Combining these, we get

$$\begin{aligned}
w(M[X]) &= w(M'[X]) \\
&\leq w(M'[X \cup Y]) \\
&\leq t_{0,X\cup Y} - \alpha_0(m) \cdot m \\
&\leq t_{1,X\cup Y} - \alpha_1(m) \cdot m - \alpha_0(m) \cdot m \\
&\vdots \\
&\leq t_{i-1,X\cup Y} - \sum_{j=0}^{i-1} \alpha_j(m) \cdot m \\
&\leq w(M[X \cup Y]) - \sum_{j=0}^{i-1} \alpha_j(m) \cdot m.
\end{aligned}$$

We rearrange this to obtain $w(M[X \cup Y]) - w(M[X]) \geq \sum_{j=0}^{i-1} \alpha_j(m) \cdot m$. ■

We can use this lemma to show that a matrix $M \in \cup_{i=1}^{g-1} C_i$ contains unavoidable patterns. To do this, let $X \in \Gamma_{\text{Qual}}$ and $i \in \mathcal{P}$ such that $Y = X \setminus i \in \Gamma_{\text{Forb}}$ and $M \in C_j$. We then have

$$w(M[Y \cup \{i\}]) - w(M[Y]) \geq \sum_{k=0}^{j-1} \alpha_k(m) \cdot m.$$

We must therefore have $\sum_{k=0}^{j-1} \alpha_k(m) \cdot m$ columns in the matrix $M[Y \cup \{i\}]$ such that there is a 1 in row i and 0 in all the other rows.

Corollary 4.6 *Let i be a strongly essential participant in a $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, g, m)$-GVCS with $i \in \Gamma_{\text{Forb}}$. For any matrix $M \in \cup_{j=0}^{g-1} C_j$, we have that*

$$w(M[\{i\}]) \geq \sum_{j=0}^{g-1} \alpha_j(m) \cdot m.$$

Proof. Choose $X \subseteq \mathcal{P}$ such that $X \cup \{i\} \in \Gamma_{\text{Qual}}$ and $X \in \Gamma_{\text{Forb}}$. From Lemma 4.5 we have that for any matrix $M \in C_{g-1}$, the matrix $M[X \cup \{i\}]$ has at least $\sum_{j=0}^{g-1} \alpha_j(m) \cdot m$ columns with a 1 in row i and 0 in the other rows. Therefore $w(M[\{i\}]) \geq \sum_{j=0}^{g-1} \alpha_j(m) \cdot m$. Additionally, since $i \in \Gamma_{\text{Forb}}$ and $X \in \Gamma_{\text{Forb}}$, Property 2 of Definition 2.5 means that this result also holds for $M' \in C_i$ for $0 \leq i \leq g-2$.■

The next lemma shows that matrices in each collection must have a certain number of columns consisting entirely of zeros. This property is necessary to distinguish the different grey levels.

Lemma 4.7 *Given $X \in \Gamma_{\text{Qual}}$ in a $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, g, m)$-GVCS. For any $M \in C_i$, the matrix $M[X]$ has at least $\sum_{j=i}^{g-2} \alpha_j(m) \cdot m$ columns with all entries equal to 0.*

Proof. From Property 1 of Definition 2.5, we have

$$\begin{aligned} w(M[X]) &\leq t_{i,X} - \alpha_i(m) \cdot m \\ &\leq t_{i+1,X} - \alpha_{i+1}(m) \cdot m - \alpha_i(m) \cdot m \\ &\vdots \\ &\leq t_{g-2,X} - \sum_{j=i}^{g-2} \alpha_j(m) \cdot m \\ &\leq m - \sum_{j=i}^{g-2} \alpha_j(m) \cdot m \end{aligned}$$

since $t_{g-2,X} \leq m$. Clearly there must be at least $\sum_{j=i}^{g-2} \alpha_j(m) \cdot m$ columns with entries all 0. ■

For an access structure $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ on a set of participants $\mathcal{P}$, given $\mathcal{P}' \subseteq \mathcal{P}$ we say that $(\Gamma'_{\text{Qual}}, \Gamma'_{\text{Forb}})$ is the *induced access structure on* $\mathcal{P}'$ to be $\Gamma'_{\text{Qual}} = \{X \in \Gamma_{\text{Qual}} : X \subseteq \mathcal{P}'\}$ and $\Gamma'_{\text{Forb}} = \{X \in \Gamma_{\text{Forb}} : X \subseteq \mathcal{P}'\}$. We have the following lemma from Atienese, Blundo, De Santis, and Stinson [1].

Lemma 4.8 *Let $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ be an access structure on $\mathcal{P}$, and let $(\Gamma'_{\text{Qual}}, \Gamma'_{\text{Forb}})$ be the induced access structure on $\mathcal{P}' \subseteq \mathcal{P}$. Then $m^*(\Gamma'_{\text{Qual}}, \Gamma'_{\text{Forb}}) \leq m^*(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$.*

This is useful to help determine the minimum pixel expansion for certain access structures where m^* is difficult to compute, but which contain an induced access structure for which m^* is easy to compute.

The following corollary follows from Lemma 2.15 and Lemma 4.8.

Corollary 4.9 *Let Γ_0 be a basis for Γ_{Qual}, and let $X \in \Gamma_0$. Then $m^*(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}) \geq (g-1)2^{|X|-1}$.*

Proof. Let $\mathcal{P}' = X$. Then $(\Gamma'_{\text{Qual}}, \Gamma'_{\text{Forb}})$ is a (k,k)-GVCS with $k = |X|$. We know from Lemma 2.15 that the optimal pixel expansion is $(g-1)2^{|X|-1}$. Applying Lemma 4.8, we obtain $m^*(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}) \geq (g-1)2^{|X|-1}$. ■

We can now use these unavoidable patterns to show that access structures arising from complete bipartite graphs have minimum pixel expansion $2(g-1)$.

Theorem 4.10 *Let $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ be an access structure with no isolated participants, and let Γ_0 be a basis for Γ_{Qual}. If there exists a GVCS with pixel expansion $2(g-1)$, then Γ_0 is the edge set of a complete bipartite graph.*

Proof. Since there are no isolated participants, we must have $|X| \geq 2$ for any $X \in \Gamma_0$. By Corollary 4.9 we have that $|X| \leq 2$ since otherwise $m \geq 4(g-1)$. Thus $|X| = 2$ for all $X \in \Gamma_0$, and Γ_0 represents the edge set of a graph G.

To show that G is connected, we will assume it is not and use a proof by contradiction. If G is not connected, then there exists a partition of $\mathcal{P}$ into $\mathcal{P}'$ and $\mathcal{P}''$ with $\mathcal{P}' \neq \emptyset$, $\mathcal{P}'' \neq \emptyset$, and $\Gamma_0 \subseteq 2^{\mathcal{P}'} \cup 2^{\mathcal{P}''}$. Let $\{i,j\} \in \Gamma_{\text{Qual}} \cap 2^{\mathcal{P}'}$ and $l \in \mathcal{P}''$. Using previous results on unavoidable patterns, we can show that for any matrix $M \in C_{g-1}$ the matrix $M[\{i,j,l\}]$ is equal, up to a column permutation, to one of the following two matrices:

$$M' = \begin{bmatrix} 1 & \dots & 1 & 0 & \dots & 0 \\ 0 & \dots & 0 & 1 & \dots & 1 \\ \underbrace{0 \;\; \dots \;\; 0}_{g-1} & & & \underbrace{1 \;\; \dots \;\; 1}_{g-1} \end{bmatrix},$$

where the first two rows are obtained using Corollary 4.6 and the third row is obtained from Lemma 4.5 setting $X = \{j, l\}$ and $Y = \{i\}$, or

$$M'' = \begin{bmatrix} 1 & \dots & 1 & 0 & \dots & 0 \\ 0 & \dots & 0 & 1 & \dots & 1 \\ \underbrace{1 \;\; \dots \;\; 1}_{g-1} & & & \underbrace{0 \;\; \dots \;\; 0}_{g-1} \end{bmatrix},$$

where the first two rows are obtained using Corollary 4.6 and the third row is obtained from Lemma 4.5 setting $X = \{i, l\}$ and $Y = \{j\}$.

Similarly $\hat{M} \in C_{g-2}$ is equal, up to a column permutation, to one of the following two matrices:

$$\hat{M}' = \begin{bmatrix} 1 & \dots & 1 & 0 & \dots & 0 & 0 & * \\ 0 & \dots & 0 & 1 & \dots & 1 & 0 & * \\ \underbrace{0 \;\; \dots \;\; 0}_{g-2} & & & \underbrace{1 \;\; \dots \;\; 1}_{g-2} & & & 0 & * \end{bmatrix}, \text{ or}$$

$$\hat{M}'' = \begin{bmatrix} 1 & \dots & 1 & 0 & \dots & 0 & 0 & * \\ 0 & \dots & 0 & 1 & \dots & 1 & 0 & * \\ \underbrace{1 \quad \dots \quad 1}_{g-2} & & & \underbrace{0 \quad \dots \quad 0}_{g-2} & & & 0 & * \end{bmatrix}.$$

We get the zero column from applying Lemma 4.7. The symbol $*$ represents an unknown value.

Thus we have

$$w(M'[\{i,l\}]) > w(\hat{M}'[\{i,l\}]);$$

$$w(M'[\{i,l\}]) > w(\hat{M}''[\{i,l\}]);$$

$$w(M''[\{j,l\}]) > w(\hat{M}'[\{j,l\}]);$$

$$w(M''[\{j,l\}]) > w(\hat{M}''[\{j,l\}]).$$

Since $\{i,l\} \in \Gamma_{\text{Forb}}$ and $\{j,l\} \in \Gamma_{\text{Forb}}$ the Hamming weights must be equal in order to satisfy Property 2. Since they are not, our assumption that G is not connected must be false and Γ_0 must be the edge-set of a connected graph.

We now prove that G is a complete multipartite graph by contradiction. We assume that G is not a complete multipartite graph. Blundo, De Santis, Stinson, and Vaccaro [4] proved that any such graph must contain as an induced subgraph which is isomorphic to H or P_3, where $V(H) = V(P_3) = \{1,2,3,4\}$, $E(H) = \{\{1,2\},\{2,3\},\{3,4\},\{2,4\}\}$, and $E(P_3) = \{\{1,2\},\{2,3\},\{3,4\}\}$.

First we will show that if G contains an induced subgraph which is isomorphic to H, we have a contradiction. K_3 is an induced subgraph of H, and represents a $(2,3)$ threshold access structure. Using unavoidable patterns we can show that there does not exist a GVCS for K_3 with pixel expansion $m = 2(g-1)$. Any matrix in C_0 must be equal, up to a column permutation, to

$$M = \begin{bmatrix} 0 \ \dots \ 0 & * \ \dots \ * \\ 0 \ \dots \ 0 & ** \ \dots \ * \\ \underbrace{0 \ \dots \ 0}_{g-1} & \underbrace{** \ \dots \ *}_{g-1} \end{bmatrix}.$$

Any matrix in C_{g-1} must be equal, up to a column permutation, to

$$M' = \begin{bmatrix} 1 \ \dots \ 1 & 1 \ \dots \ 1 \\ 0 \ \dots \ 0 & 1 \ \dots \ 1 \\ \underbrace{1 \ \dots \ 1}_{g-1} & \underbrace{0 \ \dots \ 0}_{g-1} \end{bmatrix}.$$

According to Property 2, we should have $M[\{1\}] = M'[\{1\}]$ since $\{1\} \in \Gamma_{\text{Forb}}$. Therefore there does not exist a scheme for K_3 with pixel expansion $2(g-1)$. Applying Lemma 4.8, we see that H cannot be an induced subgraph of G.

Now we show that if G contains an induced subgraph which is isomorphic to P_3 we have a contradiction. Using unavoidable patterns (Lemma 4.6), we show that any matrix in C_{g-1} must be equal, up to a column permutation, to

$$M = \begin{bmatrix} \underbrace{\begin{matrix} 1 & \dots & 1 \\ 0 & \dots & 0 \\ 1 & \dots & 1 \\ 0 & \dots & 0 \end{matrix}}_{g-1} & \underbrace{\begin{matrix} 0 & \dots & 0 \\ 1 & \dots & 1 \\ 0 & \dots & 0 \\ 1 & \dots & 1 \end{matrix}}_{g-1} \end{bmatrix}.$$

Any matrix in C_{g-2} must be equal, up to a column permutation, to

$$M' = \begin{bmatrix} \underbrace{\begin{matrix} 1 & \dots & 1 \\ 0 & \dots & 0 \\ 1 & \dots & 1 \\ 0 & \dots & 0 \end{matrix}}_{g-2} & \underbrace{\begin{matrix} 0 & \dots & 0 \\ 1 & \dots & 1 \\ 0 & \dots & 0 \\ 1 & \dots & 1 \end{matrix}}_{g-2} & \begin{matrix} 0 & * \\ 0 & * \\ 0 & * \\ 0 & * \end{matrix} \end{bmatrix}.$$

The zero column is obtained by applying Lemma 4.7.

Clearly $M[\{1,4\}] \neq M'[\{1,4\}]$, violating Property 2 since $\{1,4\} \in \Gamma_{\text{Forb}}$. Thus the access structure represented by P_3 must have $m > 2(g-1)$. By applying Lemma 4.8, the access structure represented by G must have $m > 2(g-1)$. Therefore G does not have P_3 as an induced subgraph, and G is a complete multipartite graph.

Finally, assume that G has more than 2 parts. Then G contains K_3 as an induced subgraph, and must therefore have pixel expansion $m > 2(g-1)$. Therefore G has 2 parts, and Γ_0 is the edge-set of a complete bipartite graph. ■

We can also use unavoidable patterns to show that the basis matrices of a $(3, 3)$ threshold GVCS must be of a certain form.

Theorem 4.11 *In any $(3, 3, 4(g-1), g)$-threshold GVCS, any matrix $M \in C_i$ must contain the following patterns:*

$$\left[\begin{array}{cc} 1\;\;0\;\;0\;\;1 & 0\;\;1\;\;1\;\;0 \\ 0\;\;1\;\;0\;\;1 & 0\;\;1\;\;0\;\;1 \\ \underbrace{0\;\;0\;\;1\;\;1}_{i} & \underbrace{0\;\;1\;\;1\;\;1}_{g-i-1} \end{array}\right].$$

Proof. We use induction on the number of grey levels g. The base case is where $g = 2$, which is a regular VCS. The base case clearly holds by Theorem 5.13 [1]. Assuming that it holds for k grey levels, we will show that it holds for $k + 1$ grey levels.

Both $M_0, \ldots, M_{k-1}$ and $M_1, \ldots, M_k$ constitute a GVCS on k grey levels. Combining the unavoidable patterns for these, we get the following set of matrices.

$$M_0 = \left[\begin{array}{cc} 0\;\;1\;\;1\;\;0 & *\;\;*\;\;*\;\;* \\ 0\;\;1\;\;0\;\;1 & *\;\;*\;\;*\;\;* \\ \underbrace{0\;\;0\;\;1\;\;1}_{k-1} & *\;\;*\;\;*\;\;* \end{array}\right];$$

$$M_1 = \left[\begin{array}{cc} 1\;\;0\;\;0\;\;1 & 0\;\;1\;\;1\;\;0 \\ 0\;\;1\;\;0\;\;1 & 0\;\;1\;\;0\;\;1 \\ 0\;\;0\;\;1\;\;1 & \underbrace{0\;\;1\;\;1\;\;1}_{k-1} \end{array}\right];$$

$$\vdots$$

$$M_{k-1} = \left[\begin{matrix} \underbrace{\begin{matrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{matrix}}_{k-1} & \begin{matrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{matrix} \end{matrix}\right];$$

$$M_{k} = \left[\begin{matrix} \underbrace{\begin{matrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{matrix}}_{k-1} & \begin{matrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{matrix} \end{matrix}\right].$$

We can fill in some of the missing values for M_k using unavoidable patterns:

$$M_{k} = \left[\begin{matrix} \underbrace{\begin{matrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{matrix}}_{k-1} & \begin{matrix} 1 & 0 & 0 & * \\ 0 & 1 & 0 & * \\ 0 & 0 & 1 & * \end{matrix} \end{matrix}\right].$$

Since $M_k[\{x, y\}] = M_{k-1}[\{x, y\}]$, the remaining row must consist of all 1's. Therefore we have

$$M_{k} = \left[\begin{matrix} \underbrace{\begin{matrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{matrix}}_{k-1} \end{matrix}\right].$$

Similarly for M_0, by unavoidable patterns we have

$$M_0 = \left[\begin{array}{cccccccc} 0 & 1 & 1 & 0 & 0 & * & * & * \\ 0 & 1 & 0 & 1 & 0 & * & * & * \\ \underbrace{0 \ \ 0 \ \ 1 \ \ 1}_{k-1} & & & & 0 & * & * & * \end{array} \right].$$

Since $M_0[\{x, y\}] = M_1[\{x, y\}]$, we get

$$M_0 = \left[\begin{array}{cccc} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ \multicolumn{4}{c}{\underbrace{0 \ \ 0 \ \ 1 \ \ 1}_{k-1}} \end{array} \right].$$

Therefore the theorem holds for $k + 1$ and by induction, holds for all g. Since the minimum pixel expansion for a $(3, 3)$-threshold GVCS is $4(g - 1)$, we have that any matrix $M \in C_i$ is equal, up to a column permutation, to the matrix M_i given above. ■

4.2 Graph-based Access Structures

This section gives results for access structures which are based on graphs, particularly complete graphs and complete multipartite graphs. In addition, since complete graphs are (k, n) threshold access structures with $k = 2$, we give a result for all (k, n) threshold access structures which uses generalized cover-free families.

4.2.1 A construction

It is easy to show that the rows of any matrix $M \in \cup_{i=1}^{g-1} C_i$ form a Sperner family. By Lemma 4.6, any two rows of M contain the vectors $\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$ and $\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]$. Let $G = \{g_1, \ldots, g_m\}$ and let $A_i = \{g_q : M(i,q) = 1\}$. Because of the unavoidable patterns, we have a Sperner family with n subsets over a ground set of size m. We can also use Sperner families to construct access structures based on the graph K_n, which represent $(2,n)$ threshold access structures.

Theorem 4.12 *Given a Sperner family $\mathcal{SF} = \{A_1, \ldots, A_n\}$ over a ground set $G = \{g_1, \ldots, g_m\}$, we have that $m^*(K_n) \leq m(g-1)$.*

Proof. Atienese, Blundo, De Santis, and Stinson [1] prove a similar result for regular VCS by offering a construction with pixel expansion m. They give the basis matrices

$$S_0 = \begin{cases} 1 & \text{if } 1 \leq j \leq |B_i|; \\ 0 & \text{if } |B_i| \leq j \leq m. \end{cases}$$

$$S_1 = \begin{cases} 1 & \text{if } g_j \in B_i; \\ 0 & \text{if } g_j \notin B_i. \end{cases}$$

where $1 \leq i \leq n$ and $1 \leq j \leq m$.

We will extend this to GVCS. For basis matrix G_i, simply concatenate $g - i - 1$ copies of S_0 and i copies of S_1. Since $S_0[\{i\}] = S_1[\{i\}]$ up to a column permutation (from Property 2 for VCS, since any single participant is forbidden), we must have that $G_j[\{i\}] = G_k[\{i\}]$ for any $0 \leq j, k \leq g-1$. Thus Property 2 holds. To prove Property 1, note that we have $S_1[\{i,j\}] - S_0[\{i,j\}] = d$ where d must be at least 1.

Thus if we set $t_{i,X} = w(G_{i+1}[X])$, Property 1 is satisfied with $\alpha_i(m) \cdot m = d$. The pixel expansion is therefore $m(g-1)$, so $m^*(K_n) \leq m(g-1)$. ■

4.2.2 (k,n)-threshold access structures

Access structures based on complete graphs represent $(2,n)$-threshold access structures. For this reason, we will give a more general result on (k,n)-threshold access structures, which we will use later for complete graphs. We first define generalized cover-free families. This definition is taken verbatim from Stinson and Wei [7]. First, we give some notation. A *set system* is a pair $(X, \mathcal{F})$, where X is a set of points and $\mathcal{F}$ is a set of subsets (called blocks) of X. We denote $|X|$ by N and $|\mathcal{F}|$ by T.

Definition 4.1 A set system $(X, \mathcal{F})$ is called a $(w,r;d)$-*cover-free family* (or $(w,r;d)$-CFF) provided that, for any w blocks $B_1, \ldots, B_w \in \mathcal{F}$ and any other r blocks $A_1, \ldots, A_r \in \mathcal{F}$, we have

$$\left| \left(\bigcap_{i=1}^{w} B_i \right) \setminus \left(\bigcup_{j=1}^{r} A_j \right) \right| > d,$$

where d is a non-negative integer.

We let $N((w,r;d),T)$ denote the minimum number of points for the cover-free family represented by $(w,r;d)$ and T. We have the following theorem about the relationship between (k,n)-threshold access structures and cover-free families.

Theorem 4.13 *In any (k,n)-threshold GVCS, the pixel expansion m is at least $N((1,k-1;g-2),T)$.*

Proof. Let $C_0, \ldots, C_{g-1}$ be a set of collections of matrices constituting a (k, n)-threshold GVCS with pixel expansion m and let $M \in C_{g-1}$ be any matrix. From the unavoidable patterns, for any set of k rows $\{i_1, \ldots, i_k\}$, in row i_j there are $g-1$ columns such that there is a 1 in that row and 0 in the other rows. Let $X = \{x_1, \ldots, x_m\}$ be a set of points. We can consider each row of M to be a subset of $\mathcal{F}$ where a 1 in column i indicates that point x_i is in the subset. By the unavoidable patterns, for any k rows of M, the union of any $k-1$ of the corresponding subsets does not cover (g-1) elements of the remaining subset. Thus the matrix M represents a $(1, k-1; g-2)$-CFF with $N = m$ and $T = n$, and the minimum pixel expansion is the same as the minimum number of points in the corresponding cover-free family. ■

Stinson and Wei [7] proved the following bound for $(1, r; d)$-CFF where $r \geq 2$:

$$N((1, r; d), T) \geq c \left(\frac{r^2}{\log r} \log T + dr \right),$$

where c is approximately $\frac{1}{2}$.

For the case of $(2, n)$ threshold structures, we have $r = 1$ which is a special case. We use a result about the relationship between the quantities N and T for a given d from Balding and Torney [5]. They proved:

$$T \leq \frac{1}{C_d} \binom{N}{\lfloor \frac{N}{2} \rfloor}$$

where

$$C_d = \begin{cases} 1 & \text{if } d = 0; \\ \sum_{s=0}^{d/2} \binom{\lfloor \frac{N}{2} \rfloor}{s} \binom{\lceil \frac{N}{2} \rceil}{s} & \text{if } d \text{ is even;} \\ C_{d-1} + \frac{1}{k} \binom{\lfloor \frac{N}{2} \rfloor}{(d+1)/2} \binom{\lceil \frac{N}{2} \rceil}{(d+1)/2} & \text{if } d \text{ is odd.} \end{cases}$$

and where $k = \lfloor \frac{2\lfloor N/2 \rfloor}{d+1} \rfloor$.

Thus the minimum pixel expansion is the smallest value of N satisfying $T \leq \frac{1}{C_d} \binom{N}{\lfloor \frac{N}{2} \rfloor}$.

Example 4.1 For the case where there are 4 grey levels, we can simplify the formula and give values for m^*.

$$T \leq \frac{1}{C_2} \binom{N}{\lfloor \frac{N}{2} \rfloor};$$

$$C_2 = 1 + \lfloor \frac{N}{2} \rfloor \lceil \frac{N}{2} \rceil.$$

Thus for $n = 2$, $m^* = 6$, for $n = 3, 4$, $m^* = 8$, for $n = 5$, $m^* = 9$, and for $n = 6, 7, 8, 9$, $m^* = 10$.

The following theorem holds:

Theorem 4.14 *Given a complete graph on n participants, $m^*(K_n)$ is the smallest value m such that $n \leq \frac{1}{C_{g-2}} \binom{m}{\lfloor \frac{m}{2} \rfloor}$.*

Proof. The complete graph K_n represents a $(2, n)$ threshold access structure. We can therefore use the bound given by Balding and Torney [5], and we have $m^*(K_n)$ the smallest value m such that $n \leq \frac{1}{C_{g-2}} \binom{m}{\lfloor \frac{m}{2} \rfloor}$. ■

Let $\omega(G)$ denote the maximum size of a clique in G. Then the following lemma follows from Theorem 4.14.

Lemma 4.15 *Given a graph G, there exists a $(\Gamma(G), g, m)$-GVCS only if $\omega(G) \leq \frac{1}{C_{g-2}}\binom{m}{\lfloor\frac{m}{2}\rfloor}$.*

Proof. Let G_k be the maximum size clique in G. From Theorem 4.14 we have that $m^*(G_k) = m$. Applying Lemma 4.8, the result follows. ■

We can now give the optimal pixel expansion, with a construction, for complete multipartite graphs.

Theorem 4.16 *Let $K_{a_1,\ldots,a_n}$ be a complete multipartite graph with n parts, and let $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ be the access structure it represents. There exists a $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, g, m)$-GVCS if and only if $n \leq \frac{1}{C_{g-2}}\binom{m}{\lfloor\frac{m}{2}\rfloor}$.*

Proof. First, given a $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, g, m)$-GVCS we show that $n \leq \frac{1}{C_{g-2}}\binom{m}{\lfloor\frac{m}{2}\rfloor}$. Clearly $\omega(K_{a_1,\ldots,a_n}) = n$. Thus, from Lemma 4.15 we have $n \leq \frac{1}{C_{g-2}}\binom{m}{\lfloor\frac{m}{2}\rfloor}$. ■

Given $n \leq \frac{1}{C_{g-2}}\binom{m}{\lfloor\frac{m}{2}\rfloor}$, we now give a construction for a $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, g, m)$-GVCS. Let $G_0, \ldots, G_{g-1}$ be the basis matrices of a $(\Gamma(K_n), g, m)$-GVCS. For each row q in each matrix G_i replicate row q a_q times. We now have a $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, g, m)$-GVCS.

4.2.3 Other results

These two theorems use unavoidable patterns to prove lower bounds on the pixel expansion for specific access structures.

Theorem 4.17 *Let* $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ *be a strong access structure on four participants such that* $\{1,2,4\}, \{1,3,4\} \in \Gamma_0$. *If there exists a* $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, 4(g-1), g)$*-GVCS, then there is no* $X \in \Gamma_0$ *such that* $\{2,3\} \in \Gamma_0$ *and* $\{2,3\} \in X$.

Proof. Applying Lemma 4.8, we have induced access structures $\{\{1,2,4\}\}$ and $\{\{1,3,4\}\}$. Applying Theorem 4.11, we have that any matrix $M_i \in C_i$ is equal, up to a column permutation, to

$$\left[\;\underbrace{\begin{matrix}1&0&0&1\\0&1&0&1\\0&1&0&1\\0&0&1&1\end{matrix}}_{i}\;\underbrace{\begin{matrix}0&1&1&0\\0&1&0&1\\0&1&0&1\\0&1&1&1\end{matrix}}_{g-i-1}\;\right].$$

If $\{2,3\} \subseteq X \in \Gamma_0$, then the matrix $M_i[\{2,3\}]$ must contain at least one column $\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$ and at least one column $\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]$ for all $i \geq 1$, which clearly is not true. Therefore the theorem holds. ■

Theorem 4.18 *Given* $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$*, a strong access structure on four participants with basis* $\Gamma_0 = \{\{1,2,3\}, \{1,4\}, \{3,4\}\}$*, any* $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, g, m)$*-GVCS must have* $m > 4(g-1)$.

Proof. Since $\{1,2,3\} \in \Gamma_0$, by Lemma 4.8 we must have $m \geq 4(g-1)$. Suppose there exists a GVCS with $m = 4(g-1)$. Then we must have any $M_0 \in C_0$ equal, up to a column permutation, to the following matrix.

$$\begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & * & * & * \\ \multicolumn{4}{c}{\underbrace{\qquad\qquad\qquad}_{g-1}} \end{bmatrix}$$

We have $w(M_0[\{1,2,3\}]) = w(M_0[\{2,3,4\}]) = 3(g-1)$.

In addition, we must have any $M_1 \in C_1$ equal, up to a column permutation, to the following matrix:

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ * & * & * & * & 0 & * & * & * \\ & & & & \multicolumn{4}{c}{\underbrace{\qquad\qquad\qquad}_{g-2}} \end{bmatrix}.$$

We must have $w(M_1[\{1,2,3\}]) = w(M_1[\{2,3,4\}]) = 3(g-1)+1$, and so we must have M_1 equal, up to a column permutation, to the following matrix:

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & * & 1 & * & 0 & * & * & * \\ & & & & \multicolumn{4}{c}{\underbrace{\qquad\qquad\qquad}_{g-2}} \end{bmatrix}.$$

Then there are two possibilities depending on the value of the unknowns in each matrix. If $w(M_1[\{2,4\}]) = 2(g-2)+4$, then $w(M_0[\{2,4\}]) = 2(g-1)$. If $w(M_1[\{2,4\}]) = 3(g-2)+4$, then $w(M_0[\{2,4\}]) = 3(g-1)$. Since $\{2,4\} \in \Gamma_{\text{Forb}}$, we need $w(M_1[\{2,4\}]) = w(M_0[\{2,4\}])$. We have a contradiction, therefore $m \neq 4(g-1)$, and the theorem holds. ■

Finally, we show that if there exists basis matrices for a $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$-VCS with pixel expansion m, then the minimum pixel expansion of a $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$-GVCS is at most $(g-1)m$.

Theorem 4.19 *If there exist basis matrices S_0, S_1 for a $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, m)$-VCS, then the minimum pixel expansion of a $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$-GVCS with g grey levels is $m^* \leq (g-1)m$.*

Proof. For $0 \leq i \leq g-1$ we define the basis matrices of the GVCS as follows:

$$G_i = \underbrace{S_0 \circ \ldots \circ S_0}_{g-i-1} \circ \underbrace{S_1 \circ \ldots \circ S_1}_{i}.$$

Clearly we have pixel expansion $m' = (g-1)m$. For $0 \leq i \leq g-2$, let $t_{i,X} = w(G_{i+1}[X])$ and $\alpha_i(m) = \frac{1}{(g-1)m}$. Thus, for any $X \in \Gamma_{\text{Qual}}$ we have $w(G_i[X]) \leq t_{i,X} - \alpha_i(m) \cdot m$ and $w(G_{i+1}[X]) \geq t_{i,X}$. For any $X' \in \Gamma_{\text{Forb}}$, since $S_0[X] = S_1[X]$ up to a column permutation, we have $G_0[X] = G_1[X] = \ldots = G_{g-1}[X]$ up to a column permutation. Since we have constructed a $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, (g-1)m, g-1)$-GVCS, we must have $m^* \leq (g-1)m$. ■

4.3 GVCS on four grey levels

Access structures 2, 3, 6, 7, 9, and 10 are complete multipartite graphs and the optimal pixel expansion is given by Theorem 4.16. Access structures 1, 4, 18 are (k, k)-threshold access structures and the optimal pixel expansion is given by Lemma 2.15. Lower bounds for 5, 8 are determined by Theorem 4.10. Lower bounds for 11, 13, 14 are from Corollary 4.9. Lower bounds for 15, 16, 17 are obtained from Theorem 4.17. Upper bounds for 5, 8, 11, 13, 14, 15, 16, 17 are obtained from Theorem 4.19 and the basis matrices given by Atienese, Blundo, De Santis, and Stinson [1].

access structure	n	basis subsets	m^*	result used
1	2	12	6	Lemma 2.15
2	3	12,23	6	Theorem 4.16
3	3	12,13,23	8	Theorem 4.16
4	3	123	12	Lemma 2.15
5	4	12,23,34	$7 \leq m^* \leq 9$	Theorems 4.10, 4.19
6	4	12,13,14	6	Theorem 4.16
7	4	12,14,23,34	6	Theorem 4.16
8	4	12,23,24,34	$7 \leq m^* \leq 9$	Theorems 4.10, 4.19
9	4	12,13,14,23,24	8	Theorem 4.16
10	4	12,13,14,23,24,34	8	Theorem 4.16
11	4	123,14	12	Cor. 4.9, Thm. 4.19
12	4	123,14,34	$13 \leq m^* \leq 15$	Theorems 4.18, 4.19
13	4	134,12,23,24	12	Cor. 4.9, Thm. 4.19
14	4	123,124	12	Cor. 4.9, Thm. 4.19
15	4	124,134,23	$13 \leq m^* \leq 15$	Theorems 4.17, 4.19
16	4	123,124,134	$13 \leq m^* \leq 18$	Theorems 4.17, 4.19
17	4	123,124,134,234	$13 \leq m^* \leq 18$	Theorems 4.17, 4.19
18	4	1234	24	Lemma 2.15

Table 4.1: GVCS with four grey levels for strong access structures on up to four participants

Chapter 5

Conclusions and Open Problems

We have given three constructions for GVCS on general access structures, the cumulative arrays construction, the decomposition construction, and the starting matrices construction. Of these, the decomposition construction has the most promise to result in significantly better values for the pixel expansion, assuming that the smaller access structures have good values for the pixel expansion. However, a technique for finding such a GVCS for the smaller access structures remains an open problem.

We have also given the necessary theory to give optimal values (or ranges of values) for the pixel expansion of GVCS on strong, connected access structures on at most four participants. We first showed that we need only consider connected access structures by showing how to construct a GVCS for a non-connected access structure given a GVCS for each of its connected parts. We then showed that a strong, connected GVCS must contain unavoidable patterns which are dictated by the access structure. We used these unavoidable patterns to show that for any

GVCS with pixel expansion $2(g-1)$, the access structure must be represented by a complete bipartite graph, and also to show that any $(3,3,4(g-1),4)$-threshold GVCS must have basis matrices of a particular form. We then use these results to prove optimal values for threshold access structures and access structures based on graphs. The most significant of the graph results gives the optimal pixel expansion for access structures based on complete multipartite graphs. We also give two theorems which give lower bounds on access structures containing certain sets of qualified participants, and a theorem which gives an upper bound for the pixel expansion of GVCS where there exists a corresponding VCS represented by basis matrices. Finally, we apply these results to the case of four grey levels, giving a table of values for the optimal pixel expansion of all strong, connected access structures on at most four participants.

Bibliography

[1] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis, Douglas R. Stinson. Visual cryptography for general access structures. *Information and Computation*, **129** (2), pp. 86–106, 1996.

[2] Carlo Blundo, Alfredo De Santis, Moni Naor. Visual cryptography for grey level images. *Information Processing Letters*, **75**, pp. 255–259, 2000.

[3] Carlo Blundo, Alfredo De Santis, Douglas R. Stinson. On the contrast in visual cryptography schemes. *Journal of Cryptology*, **12**, pp. 261–289, 1999.

[4] Carlo Blundo, Alfredo De Santis, Douglas R. Stinson, Ugo Vaccaro. Graph decomposition and secret sharing schemes. *Journal of Cryptology*, **8**, pp. 39-64, 1995.

[5] David J. Balding, David C. Torney. Optimal pooling designs with error detection. *Journal of Combinatorial Theory*, Series A **74**, 131-140, 1996.

[6] Moni Naor, Adi Shamir. Visual cryptography. *Eurocrypt '94*, pp. 1–12, 1994.

[7] Douglas R. Stinson, R. Wei. Generalized cover-free families. *Work in progress*, 2002.