

國立交通大學理學院應用數學系

碩士論文

以圖為基礎的存取結構上的  
秘密分享機制之研究

Perfect Secret Sharing Schemes  
for Access Structures  
Based on Graphs



研究生：林伯融

Student: Bo-Rong Lin

指導教授：傅恆霖 教授 呂惠娟 副教授

Advisor: Hung-Lin Fu and Hui-Chuan Lu

中華民國一百零三年六月

June, 2014

# Perfect Secret Sharing Schemes for Access Structures Based on Graphs

## 以圖為基礎的存取結構上的 秘密分享機制之研究

研究生：林伯融  
指導教授：傅恆霖 教授  
呂惠娟 副教授

Student：Bo-Rong Lin  
Advisor：Hung-Lin Fu  
Hui-Chuan Lu



A Dissertation

Submitted to Department of Applied Mathematics  
College of Science

National Chiao Tung University  
in Partial Fulfillment of the Requirements  
for the Degree of Master  
in Applied Mathematics

June 2014  
Hsinchu, Taiwan, Republic of China

中華民國一百零三年六月

June, 2014

## 摘要

秘密分享機制 (secret sharing scheme) 是一個將秘密分成許多份 (share) 分給所有的參與者，使得只有特定被授權的子集 (qualified subset) 中的人所擁有的 shares 才可以重新建構出這個秘密；而任意非授權子集中的人，則無法由他們所擁有的 shares 中找出任何與秘密相關的資訊的一種機制。其中，所有的授權子集所形成的集合我們稱之為該機制的存取結構 (access structure)。

所謂以一個圖  $G$  為基礎的存取結構，是將圖  $G$  上每一個點都視為一個參與者，而任意一個包含某個邊的一些點所成的集合都是一個授權的子集。其中秘密分享機制的訊息比率 (information ratio) 則是該秘密分享機制下所有參與者所擁有的 shares 的最大長度與秘密的長度的比值。而我們在這篇論文中所討論圖  $G$  的訊息比率 (information ratio of  $G$ ) 則是在以圖  $G$  為基礎的存取結構中所能造出的所有秘密分享機制的訊息比率的 infimum。

在這篇論文中，我們求出了特定無窮圖類的訊息比率的下界，並且利用向量空間的方式，完整造出這特定無窮圖類中兩種特殊子圖類的秘密分享機制，並算出其訊息比率的值皆為 2。如此便得出這二種子圖類的訊息比率的上界。在某些情形下，此上界與我們推導的下界是相當接近的，亦即我們構造的秘密分享機制是相當好的。

# Abstract

A perfect secret sharing scheme based on a graph  $G$  is a randomized distribution of a secret among the vertices of the graph so that the secret can be recovered from the information assigned to the endvertices of any edge, while the total information assigned to an independent set of vertices is independent (in statistical sense) of the secret itself.

The (worst case) *information ratio* of  $G$  is the largest lower bound on the amount of information some vertex must remember for each bit of the secret. Using entropy method, we calculate a lower bound on the information ratio for an infinite class of graphs we consider in this thesis. We also use the generalized vector space construction to construct perfect secret sharing schemes with information ratio 2 for two subclasses of graphs. This upper bounded is very close to our lower bound in some circumstances, which means the secret sharing schemes we construct are in fact very good.

## 誌謝

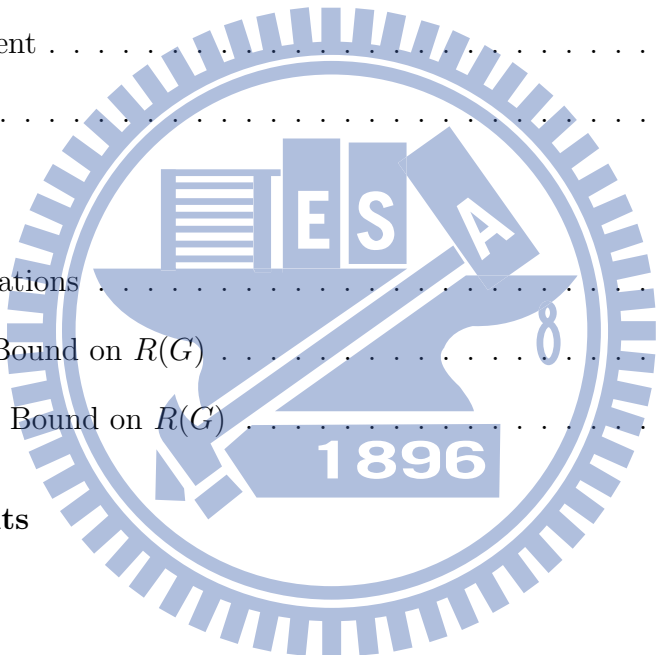
這篇論文能夠完成，首先要感謝的是我指導老師 傅恆霖教授還有 呂惠娟副教授，感謝傅老師從一開始就提供我一些往後研究可能會使用到的工具書去研讀，還建議我研究的大方向並且介紹呂老師來幫助我完成論文。感謝呂老師在每次要討論有關於我的研究時，都大老遠開車來交大，並給予我許多的啟發與收穫，在最後幾週更提供專業的意見和細心的修改我論文的每一個部分，讓我的論文更加的充實。

此外我還要感謝同門的才維瀚學長、施智懷學長、林逸軒學長、連敏筠學姊，在我每次報告的時候，都不吝嗇的給予建議、指導，在口試前也都空出時間來幫助我模擬口試，讓我可以調整口試內容，也謝謝我的同學惠閔、伊婕、冠儒、博喻、凡軒、凱帆，記得每次都一起討論作業到半夜，還有每次聚餐都開心的亂聊天，另外還有交大數學系的系羽接納我這個外來的學長，讓我可以課業之餘還可以打球來放鬆一下。

最後感謝我的家人，不會強迫我做任何事情，並且一直關心和照顧我，在我需要時也都會適時的伸出援手，讓我可以專注於課業與研究。在此至上我最大的感激，謝謝你們！

# Contents

Abstract (in Chinese) . . . . .	i
Abstract (in English) . . . . .	ii
Acknowledgement . . . . .	iii
Contents . . . . .	iv
<b>1 Introduction</b>	<b>1</b>
1.1 Basic Notations . . . . .	2
1.2 A Lower Bound on $R(G)$ . . . . .	3
1.3 An Upper Bound on $R(G)$ . . . . .	4
<b>2 Known Results</b>	<b>6</b>
<b>3 Main Results</b>	<b>9</b>
3.1 A Lower Bound on $R(G_{k,n})$ . . . . .	10
3.2 A Construction of Perfect Secret Sharing Scheme on $G'_{k,n}$ . . . . .	13
3.3 A Construction of Perfect Secret Sharing Scheme on $G''_{k,n}$ . . . . .	18
3.4 Concluding Remark . . . . .	22



# Chapter 1

## Introduction

Secret sharing scheme is a method for a dealer to distribute a secret data among a set of participants so that only qualified subsets are able to recover the data. If, in addition, unqualified subsets have no extra information, i.e. their joint shares is statistically independent of the secret, the scheme is called *perfect*. The access structure of the scheme is the collection of all qualified subsets. When the access structure is based on a graph, the vertices of the graph are the participants, and if a collection of vertices contains an edge, then it is qualified. The efficiency of a scheme is usually measured by how much information (in bits) a participant must remember in the scheme in the worst case, or in the average. The (worst case) *information ratio* of a graph  $G$  is the infimum of the information (in bits) a participant has to remember for each bit of the secret over all possible schemes based on  $G$ . In some literatures, the inverse of this number, called the information rate of  $G$ , is used in resemblance to the coding efficiency on noisy channels.

Determining the information ratio for a simple graph could be very challenging. Despite the difficulty, the ratios were exactly determined for several infinite families of graphs [4, 11, 12, 13]. Interestingly, almost all of these ratios are of the forms  $2 - 1/k$  or  $3/2$  for some positive integer  $k$ . In this thesis we investigate the information ratio of another family of graphs. Our lower bound on the information ratio of this family

of graphs is also of the form  $2 - \frac{1}{k}$  for some integer  $k$ .

This thesis is organized as follows. In the rest sections of this chapter, we introduce our approaches for deriving lower bounds and upper bounds on  $R(G)$ . In Chapter 2, some important known results are introduced. Our main results are presented in Chapter 3. First, in Section 3.1, we propose an infinite class of graphs  $G_{k,n}$ , and then use the idea introduced in Section 1.2 to derive a lower bound on the information ratio of them. Subsequently, the constructions of the secret sharing schemes based on two subclasses of these graphs with information ratio 2 are introduced. The information ratio of our constructions is very closed to the lower bound we derive in Section 3.1 for large  $n$ . A concluding remark will be given in Section 3.4.

## 1.1 Basic Notations

Let  $G$  be a graph. A secret sharing scheme for the access structure base on  $G$  is a collection of random variable  $\zeta_s$  and  $\zeta_v$  for all vertices  $v$  in  $G$  with a joint distribution, where  $\zeta_s$  is the secret and  $\zeta_v$  is the share of  $v$ . We called the secret sharing scheme perfect whenever the following condition is satisfied. If  $vu$  is an edge of  $G$ , then  $\zeta_v$  and  $\zeta_u$  together determine the value of the secret  $\zeta_s$  uniquely; while if  $A$  is an independent set in  $G$ , then the collection  $\{\zeta_v : v \in A\}$  and  $\zeta_s$  are statistically independent, i.e. the collection  $\{\zeta_v : v \in A\}$  provides no information about the secret.

Let  $A$  and  $B$  be two sets. We use  $AB$  in place of  $A \cup B$  in this thesis. Using the usual (Shannon) entropy [9],  $A$  determines  $B$  if and only if the entropy of  $A$  and the entropy of  $AB$  are the same, while  $A$  and  $B$  are statistically independent if and only if the entropy of  $AB$  is the sum of the entropy of  $A$  and the entropy of  $B$ . Given a discrete random variable  $X$  with possible values  $\{x_1, x_2, \dots, x_n\}$  and a probability distribution  $\{p(x_i)\}_{i=1}^n$ , the Shannon entropy is defined as  $H(X) =$



$-\sum_{i=1}^n p(x_i) \log p(x_i)$  which is roughly the number of independent bits necessary to encode the value of  $X$ . Applying this notation to secret sharing we see that the size of the share assigned to the participant  $v \in G$  is  $H(\zeta_v)$ , and the size of the secret is  $H(\zeta_s)$ . Thus the information ratio of the secret sharing scheme  $\Sigma = \{\zeta_s, \zeta_v : v \in V(G)\}$  on  $G$  is defined as

$$R_\Sigma = \frac{\max_{v \in G} H(\zeta_v)}{H(\zeta_s)},$$

and the information ratio of  $G$  is defined as

$$R(G) = \inf \left\{ R_\Sigma : \Sigma \text{ is a secret sharing scheme on } G \right\}.$$

## 1.2 A Lower Bound on $R(G)$

Let the distribution  $\{\zeta_v, \zeta_s\}$  be any perfect secret sharing scheme on  $G$ . Consider the real-valued function  $f$  which assigns the value

$$f(A) = \frac{H(\{\zeta_v : v \in A\})}{H(\zeta_s)}$$

to the subset  $A$  of vertices. Using standard properties of the entropy function [9, 10, 14], the function  $f$  has the following properties.

- (a)  $f(A) \geq 0, f(\emptyset) = 0$
- (b)  $f(B) \geq f(A)$ , when  $A \subseteq B \subseteq V(G)$
- (c)  $f(A) + f(B) \geq f(A \cup B) + f(A \cap B)$
- (d)  $f(B) \geq f(A) + 1$ , when  $A \subseteq B \subseteq V(G)$ ,  $A$  is an independent set and  $B$  is not.
- (e)  $f(A) + f(B) \geq f(A \cup B) + f(A \cap B) + 1$ , when  $A \cap B$  is an independent set but  $A$  and  $B$  are not.

Suppose there exists a real number  $r$  so that, for any real-valued function  $f$  satisfying properties (a) to (e), the inequality  $\max_{v \in G} f(v) \geq r$  holds. Then, the information ratio  $R(G)$  of  $G$  is at least  $r$ .

### 1.3 An Upper Bound on $R(G)$

Upper bounds are in general easier to find. One has to construct an appropriate scheme which reaches the given bound. We use some algebraic or geometric structures to build up the desired scheme. The following construction is a general one given in [6].

Let  $\mathbb{F}$  be a finite-dimensional vector space over a finite field, and the secret and the participants are both (non-trivial) linear subspaces of  $\mathbb{F}$ . Let  $L_v$  be the subspace assigned to  $v \in G$  and  $L_s$  be the subspace assigned to the secret. These subspaces should have the following properties:

- (i) If  $vu$  is an edge in  $G$ , then the linear span of  $L_v$  and  $L_u$  must contain  $L_s$ .
- (ii) If  $\{v_1, v_2, \dots, v_k\}$  is an independent set of  $G$ , then the intersection of the linear span of  $\{L_{v_1}, L_{v_2}, \dots, L_{v_k}\}$  and  $L_s$  must be trivial. (i.e. the single element subspace  $\{0\}$ .)

The dealer chooses an element from  $\mathbb{F}$  randomly. The secret, i.e. the value of  $\zeta_s$ , is the orthogonal projection of this random element on  $L_s$ . The value of the share  $\zeta_v$  of participant  $v \in G$  is the orthogonal projection of the dealer's element on  $L_v$ .

Now, if  $vu$  is an edge of  $G$ , by elementary linear algebra, we know that the secret can be expressed as an appropriate linear combination of the shares. On the other hand, if  $\{v_1, v_2, \dots, v_k\}$  is an independent set of  $G$ , then the intersection of the linear span of  $\{L_{v_1}, L_{v_2}, \dots, L_{v_k}\}$  and  $L_s$  is  $\{0\}$ . Therefore, the projection on the first one

gives no information at all on the value of projection on the other.

Looking at this construction more carefully, the function  $f$  defined in Section 1.2 takes the same value as the ratio of the the dimensions of the corresponding subspaces, that is,

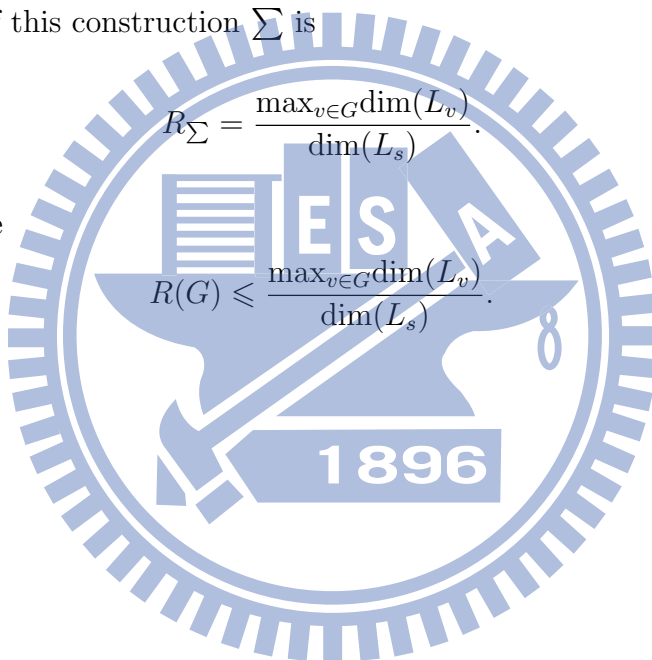
$$f(A) = \frac{H(\{\zeta_v : v \in A\})}{H(\zeta_s)} = \frac{\dim(\langle L_v : v \in A \rangle)}{\dim(L_s)}.$$

The amount of information (i.e. entropy) in the secret is proportional to the dimension of  $L_s$ , and the information  $v$  gets is proportional to the dimension of  $L_v$ . Hence, the ratio of this construction  $\Sigma$  is

$$R_\Sigma = \frac{\max_{v \in G} \dim(L_v)}{\dim(L_s)}.$$

Therefore, we have

$$R(G) \leq \frac{\max_{v \in G} \dim(L_v)}{\dim(L_s)}.$$



# Chapter 2

## Known Results

In this chapter, we introduce several lemmas and known results.

**Theorem 2.1.** ([2]) *Suppose that  $G$  is a connected graph, then  $R(G) = 1$  if and only if  $G$  is a complete multipartite graph.*

**Lemma 2.2.** ([3]) *Suppose that  $u$  and  $v$  are two vertices of a graph  $G$  who have the same neighbors, then  $R(G) = R(G - v)$ .*

**Theorem 2.3.** ([1]) *Let  $G$  be a graph with  $V(G) = \{v_i | i = 1, 2, \dots, 4\}$ . If  $v_1v_2, v_2v_3, v_3v_4 \in E(G)$  and  $v_1v_4, v_1v_3 \notin E(G)$ . Then  $R(G) \geq \frac{3}{2}$ .*

van Dijk also used this approach to characterize graphs of order six whose information ratio is not less than  $\frac{5}{3}$ .

**Theorem 2.4.** ([12]) *Let  $G$  be a graph with  $V(G) = \{v_i | i = 1, 2, \dots, 6\}$ .*

*If  $G$  satisfies both*

- (i)  $v_1v_2, v_3v_4, v_5v_6 \in E(G)$  and
- (ii)  $v_1v_5, v_1v_6, v_2v_5, v_2v_6, v_3v_5, v_3v_6 \notin E(G)$

*and at least one of the following conditions.*

- $v_2v_4, v_4v_6 \in E(G)$

- $v_2v_3, v_3v_4 \in E(G)$
- $v_2v_3, v_2v_4 \in E(G)$  or
- $v_3v_4, v_2v_4 \in E(G)$

Then  $R(G) \geq \frac{5}{3}$ .

**Lemma 2.5.** ([1]) If  $G'$  is an induced subgraph of a graph  $G$ , then  $R(G) \geq R(G')$ .

**Theorem 2.6.** ([1]) Suppose that  $G$  is a connected graph which is not complete multipartite, then  $R(G) \geq \frac{3}{2}$ .

**Theorem 2.7.** ([11]) Let  $C_n$  and  $P_n$  be the cycle and the path of length  $n$ , respectively. Then

$$R(C_n) = \frac{3}{2} \text{ for } n \geq 5, \text{ and}$$

$$R(P_n) = \frac{3}{2} \text{ for } n \geq 3.$$

**Theorem 2.8.** ([5]) Let  $G_i \subseteq G$  be arbitrary (finite or infinite) subgraphs of  $G$ , and assume that each edge of  $G$  is in at least  $k$  of the subgraphs. For a vertex  $v \in G$  define  $r_i(v) = 0$  if  $v \notin G_i$ , and  $r_i(v) = R(G_i)$ , i.e. the information ratio of  $G_i$  otherwise. Then

$$R(G) \leq \sup_{v \in G} \frac{\sum r_i(v)}{k}.$$

**Corollary 2.9.** ([5]) If the maximal degree of  $G$  is  $d$ , then  $R(G) \leq (d + 1)/2$ .

The following lemma will be frequently used in Section 3.1.

**Lemma 2.10.** ([6]) Let  $X$  be a subset of an independent set  $W$ ,  $w \in W - X$ ,  $a, b \in V$ , where  $V$  is the vertex set of a complete graph with  $n$  vertices, so that  $a$  is not connected to any vertex in  $X \cup \{w\}$ , while  $b$  is connected to  $w$ . Then

$$f(\{a\} \cup X) - f(X) + f(\{b\} \cup X) - f(X) \geq f(\{a, w\} \cup X) - f(\{w\} \cup X) + 2.$$

A subset  $V_0$  of  $V(G)$  is called connected if it induces a connected subgraph of  $G$ . Csirmaz and Tardas [8] defined a core  $V_0$  of a graph  $G$  as a connected subset  $V_0$  of  $G$  satisfying the following two conditions:

- (i) each  $v \in V_0$  has a neighbor  $\bar{v}$  outside  $V_0$  and is not adjacent to any other vertices in  $V_0$ , and
- (ii)  $\{\bar{v} | v \in V_0\}$  is an independent set in  $G$ .

They had an important breakthrough on the study of the information ratio of graphs in 2007.

**Theorem 2.11.** ([8]) *Let  $c(T)$  be the maximum size of a core in the tree  $T$ , then*

$$R(T) = 2 - \frac{1}{c(T)}.$$

In 2009, Csirmaz and Ligeti [7] proved the following result which is so far the best on the information ratio of graphs.

**Theorem 2.12.** [7] *Let  $d$  be the maximum degree of  $G$  and  $G$  satisfy the following properties:*

- (i) every vertex has at most one neighbor of degree one;
- (ii) vertices of degree at least three are not connected by an edge, and
- (iii) the girth of  $G$  is at least six.

Then we have

$$R(G) = 2 - \frac{1}{d}.$$

# Chapter 3

## Main Results

Throughout of this chapter we let  $G_{k,n}$  be the graph with vertex set  $V(G_{k,n}) = \{v_{i,j} | i = 1, 2, \dots, k, j = 1, 2, \dots, n\} \cup \{w_1, w_2, \dots, w_n\}$  and satisfy the following conditions.

- (1)  $v_{i,j}v_{i,m}$  is an edge of  $G_{k,n}$  for each  $i \in \{1, 2, \dots, k\}$  and  $j \in \{1, 2, \dots, n\}$ ;
- (2)  $w_j$  is only connected to  $v_{i,j}$  for each  $i$  and  $j$ .

Let us denote the set of vertices  $\{v_{i1}, v_{i2}, \dots, v_{in}\}$  as  $V_i$  for each  $i \in \{1, 2, \dots, k\}$  and  $\{w_1, w_2, \dots, w_n\}$  as  $W$ . Then the subgraph induced by  $V_i$  is a complete graph and  $W$  is an independent set in  $G_{k,n}$ . For clearness, we show the structure of  $G_{3,4}$ , in figure 3.1.

Note that in such a graph  $G_{k,n}$ , there may be some edges between  $V_i$ 's. No matter whether  $G_{k,n}$  contains such edges or not, the derivation of the lower bound in Section 3.1 works. In addition, we use  $G'_{k,n}$  to denote the graph  $G_{k,n}$  which contains all edges of the form  $v_{i,j}v_{\ell,m}$  for all  $i, \ell \in \{1, 2, \dots, k\}$  and  $j, m \in \{1, 2, \dots, n\}$ . The  $G_{k,n}$  which contains no edges between different  $V_i$ 's is written as  $G''_{k,n}$ . We shall introduce the constructions of perfect secret sharing schemes for graphs  $G'_{k,n}$  and  $G''_{k,n}$  in Section 3.2 and Section 3.3 respectively.

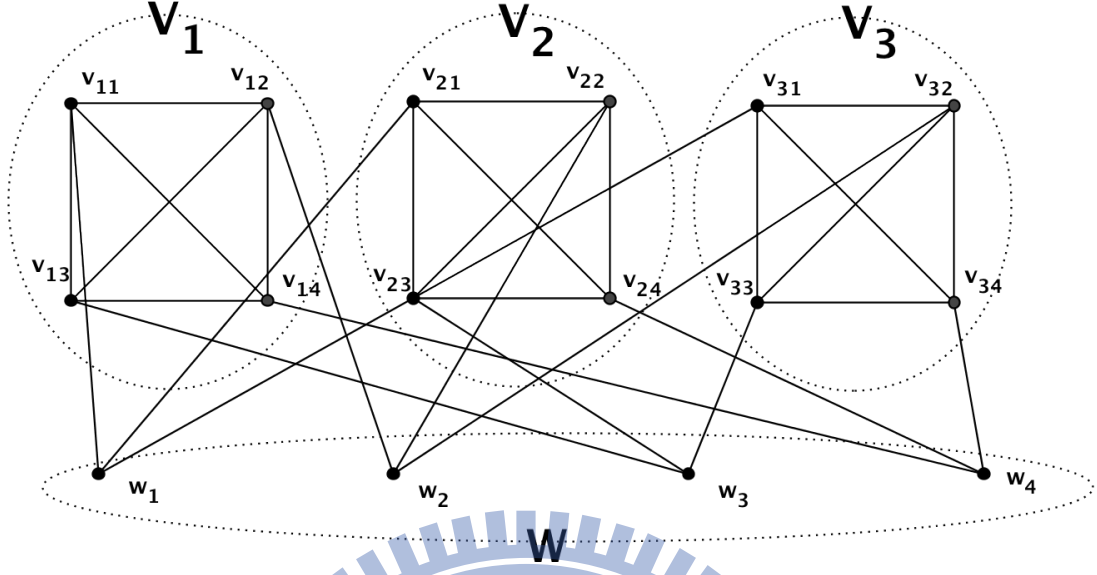


Figure 3.1:  $G_{3,4}$

### 3.1 A Lower Bound on $R(G_{k,n})$

Let  $f$  be the real-valued function defined in Section 1.2 which assigns non-negative values to subsets of vertices so that  $f$  satisfies properties (a)-(e) listed there. Our goal is to give the best possible lower estimate for  $\max_{v \in V(G)} f(v)$ . We will use Lemma 2.10. to prove that the the information ratio of the graph  $G_{k,n}$  is not less than  $2 - 2^{-n+1}$ .

As it is customary, we leave out the  $\{\}$  and  $\cup$  signs in the following discussion. For example, we write  $vX$  for the set  $\{v\} \cup X$ .

**Theorem 3.1.**  $R(G_{k,n}) \geq 2 - 2^{-n+1}$ .

**Proof.** For every  $i \in \{1, 2, \dots, k\}$  and  $j \in \{1, 2, \dots, n\}$ , using Lemma 2.10 with  $X = \{\phi\}$ ,  $a = v_{i,j}$ ,  $b = v_{i1}$ ,  $w = w_1$ , we get

$$f(v_{i2}) + f(v_{i1}) \geq f(v_{i2}w_1) - f(w_1) + 2 \text{ and}$$

$$f(v_{i,j}) + f(v_{i1}) \geq f(v_{i,j}w_1) - f(w_1) + 2, \text{ where } 3 \leq j \leq n.$$



Adding up these inequalities, we have

$$f(v_{i,j}) + f(v_{i2}) + 2f(v_{i1}) \geq f(v_{i,j}w_1) - f(w_1) + f(v_{i2}w_1) - f(w_1) + 2 + 2,$$

where  $3 \leq j \leq n$ .

Applying Lemma 2.7 to the right hand side of the inequality leads to

$$f(v_{i3}) + f(v_{i2}) + 2f(v_{i1}) \geq f(v_{i3}w_2w_1) - f(w_2w_1) + 2 + 2 \cdot 2 \text{ and}$$

$$f(v_{i,j}) + f(v_{i2}) + 2f(v_{i1}) \geq f(v_{i,j}w_2w_1) - f(w_2w_1) + 2 + 2 \cdot 2, \text{ where } 4 \leq j \leq n.$$

Adding up these inequalities and using Lemma 2.7 again, we get

$$f(v_{i4}) + f(v_{i3}) + 2f(v_{i2}) + 4f(v_{i1}) \geq f(v_{i4}w_3w_2w_1) - f(w_3w_2w_1) + 2 + 2 \cdot 2 + 2 \cdot 2^2$$

and

$$f(v_{i,j}) + f(v_{i3}) + 2f(v_{i2}) + 4f(v_{i1}) \geq f(v_{i,j}w_3w_2w_1) - f(w_3w_2w_1) + 2 + 2 \cdot 2 + 2 \cdot 2^2$$

, where  $5 \leq j \leq n$ .

Continuously doing this process, we will eventually arrive at the following inequality.

$$\begin{aligned} & f(v_{in}) + f(v_{i(n-1)}) + 2f(v_{i(n-2)}) + 2^2f(v_{i(n-3)}) + \cdots + 2^{n-3}f(v_{i2}) + 2^{n-2}f(v_{i1}) \\ & \geq f(v_{in}w_{n-1} \cdots w_2w_1) - f(w_{n-1} \cdots w_2w_1) + 2 + 2 \cdot 2 + \cdots + 2 \cdot 2^{n-2} \\ & \geq f(v_{in}w_{n-1} \cdots w_2w_1) - f(w_{n-1} \cdots w_2w_1) + 2(2^{n-1} - 1). \end{aligned}$$

Let  $S = \{w_{n-1} \cdots w_2w_1\}$ . Conditions (c) and (d) imply that

$$f(v_{in}S) + f(w_nS) \geq f(v_{in}w_nS) + f(S)$$

and

$$f(v_{in}w_nS) \geq f(w_nS) + 1.$$

Adding these up and transpose  $f(S)$  we have

$$f(v_{in}S) - f(S) \geq 1.$$

Hence,

$$f(v_{in}w_{n-1} \cdots w_2w_1) - f(w_{n-1} \cdots w_2w_1) + 2(2^{n-1} - 1) \geq 1 + 2(2^{n-1} - 1) = 2^n - 1.$$

Consequently,

$$f(v_{in}) + f(v_{i(n-1)}) + 2f(v_{i(n-2)}) + \cdots + 2^{n-2}f(v_{i1}) \geq 2^n - 1.$$

Observe that the inequality remain true after shifting vertices in  $V_i$ , that is

$$f(v_{in}) + f(v_{i(n-1)}) + 2f(v_{i(n-2)}) + \cdots + 2^{n-3}f(v_{i2}) + 2^{n-2}f(v_{i1}) \geq 2^n - 1,$$

$$f(v_{i(n-1)}) + f(v_{i(n-2)}) + 2f(v_{i(n-3)}) + \cdots + 2^{n-3}f(v_{i1}) + 2^{n-2}f(v_{in}) \geq 2^n - 1,$$

$$f(v_{i1}) + f(v_{in}) + 2f(v_{i(n-1)}) + \cdots + 2^{n-3}f(v_{i3}) + 2^{n-2}f(v_{i2}) \geq 2^n - 1.$$

Adding them up, each  $f(v_{i,j})$  will have coefficient

$$1 + 1 + 2 + 4 + \cdots + 2^{n-2} = 2^{n-1},$$

hence the sum is

$$2^{n-1}[f(v_{i1}) + f(v_{i2}) + \cdots + f(v_{in})] \geq n(2^n - 1), \quad \text{for all } i = 1, 2, \dots, k.$$

Therefore,

$$2^{n-1} \sum_{i=1}^k \sum_{j=1}^n f(v_{i,j}) \geq nk(2^n - 1).$$

There must exist a vertex whose value is not less than  $(2^n - 1)/2^{n-1} = 2 - 2^{-n+1}$ .

The proof is complete. □

## 3.2 A Construction of Perfect Secret Sharing Scheme on $G'_{k,n}$

In this section we introduce our construction of perfect secret sharing scheme on  $G'_{k,n}$  whose information ratio is equal to 2.

Our constructions follow the ideal outlined in Section 1.3. In order to construct a perfect secret sharing scheme with ratio  $\max_{v \in G} \dim(L_v) / \dim(L_s)$ , we start with a high-dimensional vector space  $\mathbb{F}$ , and assign linear subspaces to the vertices and the secret so that

- if  $vu$  is an edge of the graph, then the linear span of the subspaces  $L_v$  and  $L_u$  contains the subspace  $L_s$  which is assigned to the secret, and
- if  $\{v_1, v_2, \dots, v_k\}$  is an independent set, then  $\text{Span}(\{L_{v_1}, L_{v_2}, \dots, L_{v_k}\}) \cap L_s = \{0\}$ .

In our construction,  $\mathbb{F}$  is a  $d(kn + 1)$ -dimensional vector space and subspaces will be given as the linear span of certain vectors. We split these coordinates into  $kn + 1$  groups of  $d$  coordinates each. Now, we need some more definition and notation to help us describe our construction. If  $x$  and  $y$  are two  $\ell$ -dimensional vectors, then  $x^k$  is defined as the  $k\ell$ -dimensional vector obtained by repeating the coordinates of  $x$   $k$  times. The vector  $x \oplus y$  is  $2\ell$ -dimensional vector obtained by concatenating vector  $y$  after  $x$ . For example, if  $x = (010)$  and  $y = (101)$ , then  $x^3 = (010010010)$  and  $y \oplus x^2 = (101010010)$ .

**Construction 3.2.** Let  $\lambda_1, \lambda_2, \dots, \lambda_{km}$  be  $km$  distinct integers, and let  $\lambda_x - \lambda_y$  be denoted as  $\lambda_{x,y}$ .

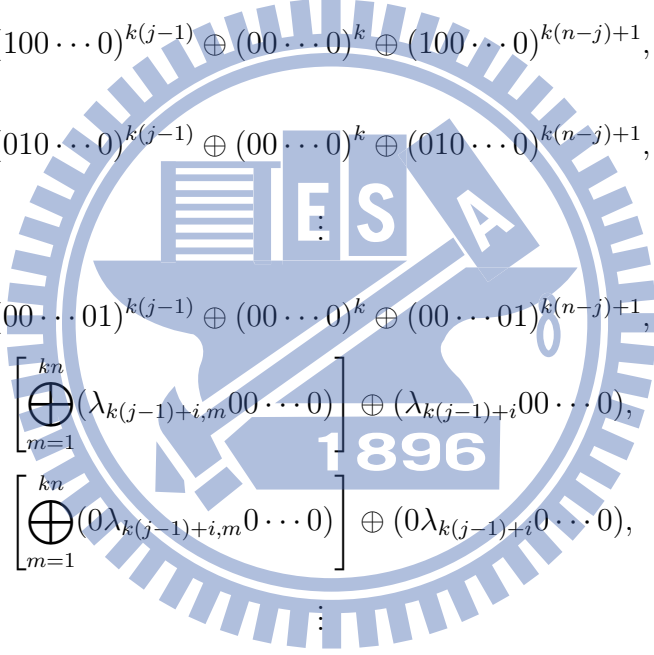
The subspace  $L_s$  assigned to the secret is spanned by the following  $d$  vectors:

$$(1000 \dots 0)^{kn+1}, (0100 \dots 0)^{kn+1}, (0010 \dots 0)^{kn+1}, \dots, (000 \dots 01)^{kn+1}.$$

The subspace  $L_{w_j}$  assigned to  $w_j$  is spanned by the following  $d$  vectors:

$$\begin{aligned}
& (0 \dots 0)^{k(j-1)} \oplus (100 \dots 0)^k \oplus (0 \dots 0)^{k(n-j)+1}, \\
& (0 \dots 0)^{k(j-1)} \oplus (010 \dots 0)^k \oplus (0 \dots 0)^{k(n-j)+1}, \\
& \quad \vdots \\
& (0 \dots 0)^{k(j-1)} \oplus (00 \dots 01)^k \oplus (0 \dots 0)^{k(n-j)+1}.
\end{aligned}$$

Furthermore, the subspace  $L_{v_{i,j}}$  assigned to  $v_{i,j}$  is spanned by the following  $2d$  vectors:



$$\begin{aligned}
& (100 \dots 0)^{k(j-1)} \oplus (00 \dots 0)^k \oplus (100 \dots 0)^{k(n-j)+1}, \\
& (010 \dots 0)^{k(j-1)} \oplus (00 \dots 0)^k \oplus (010 \dots 0)^{k(n-j)+1}, \\
& (00 \dots 01)^{k(j-1)} \oplus (00 \dots 0)^k \oplus (00 \dots 01)^{k(n-j)+1}, \\
& \left[ \bigoplus_{m=1}^{kn} (\lambda_{k(j-1)+i,m} 00 \dots 0) \right] \oplus (\lambda_{k(j-1)+i} 00 \dots 0), \\
& \left[ \bigoplus_{m=1}^{kn} (0 \lambda_{k(j-1)+i,m} 0 \dots 0) \right] \oplus (0 \lambda_{k(j-1)+i} 0 \dots 0), \\
& \quad \vdots \\
& \left[ \bigoplus_{m=1}^{kn} (00 \dots 0 \lambda_{k(j-1)+i,m}) \right] \oplus (00 \dots 0 \lambda_{k(j-1)+i}).
\end{aligned}$$

Figure 3.2 shows the graphs  $G'_{2,2}$  and we give our construction of secret sharing scheme on it in Example 3.3.

**Example 3.3.**

$$L_s = \text{Span}\{(100100100100100), (010010010010010), (001001001001001)\}$$

$$L_{w_1} = \text{Span}\{(100100000000000), (010010000000000), (000000000000000)\}$$

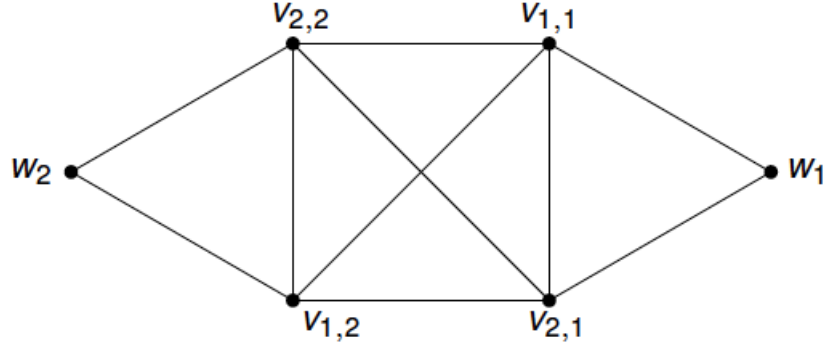


Figure 3.2:  $G'_{2,2}$

$$L_{w_2} = \text{Span}\{(000000100100000), (000000010010000), (000000001001000)\}$$

$$L_{v_{1,1}} = \text{Span}\{(000000100100100), (000000010010010), (000000001001001),$$

$$(\lambda_{1,1}00\lambda_{1,2}00\lambda_{1,3}00\lambda_{1,4}00\lambda_100), (0\lambda_{1,1}00\lambda_{1,2}00\lambda_{1,3}00\lambda_{1,4}00\lambda_10),$$

$$(00\lambda_{1,1}00\lambda_{1,2}00\lambda_{1,3}00\lambda_{1,4}00\lambda_1)\}$$

$$L_{v_{2,1}} = \text{Span}\{(000000100100100), (000000010010010), (000000001001001),$$

$$(\lambda_{2,1}00\lambda_{2,2}00\lambda_{2,3}00\lambda_{2,4}00\lambda_200), (0\lambda_{2,1}00\lambda_{2,2}00\lambda_{2,3}00\lambda_{2,4}00\lambda_20),$$

$$(00\lambda_{2,1}00\lambda_{2,2}00\lambda_{2,3}00\lambda_{2,4}00\lambda_2)\}$$

$$L_{v_{1,2}} = \text{Span}\{(100100000000100), (010010000000010), (0010010000000001),$$

$$(\lambda_{3,1}00\lambda_{3,2}00\lambda_{3,3}00\lambda_{3,4}00\lambda_300), (0\lambda_{3,1}00\lambda_{3,2}00\lambda_{3,3}00\lambda_{3,4}00\lambda_30),$$

$$(00\lambda_{3,1}00\lambda_{3,2}00\lambda_{3,3}00\lambda_{3,4}00\lambda_3)\}$$

$$\begin{aligned}
L_{v_2,2} = \text{Span}\{ & (100100000000100), (010010000000010), (001001000000001), \\
& (\lambda_{4,1}00\lambda_{4,2}00\lambda_{4,3}00\lambda_{4,4}00\lambda_{4,0}), (0\lambda_{4,1}00\lambda_{4,2}00\lambda_{4,3}00\lambda_{4,4}00\lambda_{4,0}), \\
& (00\lambda_{4,1}00\lambda_{4,2}00\lambda_{4,3}00\lambda_{4,4}00\lambda_{4,0})\}
\end{aligned}$$

**Theorem 3.4.** *Constriction 3.2. defines a perfect secret sharing scheme on  $G'_{k,n}$  with information 2.*

**Proof.** To show that Construction 3.2. is a perfect secret sharing scheme on  $G'_{k,n}$ , we need to check the following conditions.

1. the span of  $L_{w_1}, L_{w_2}, \dots, L_{w_n}$  must be trivial,
2. the span of  $L_{v_{i,j}}$  and  $L_{w_j}$  must contain  $L_s$ ,
3. the span of  $L_{v_{i,j}}$  and  $\{L_{w_m} : m \neq j\}$  intersects  $L_s$  in the trivial space  $\{0\}$ , and
4. the span of two different  $L_{v_{i,j}}$  and  $L_{v_{m,n}}$  should contain  $L_s$ .

Since the linear span of all subspaces  $L_{w_j}$ 's contains those vectors where all coordinates in the  $(kn + 1)$ -th group are zero and any non-trivial linear combination of  $L_s$  has non-zero coordinates in each group, we have

$$\text{Span}\{L_{w_1}, L_{w_2}, \dots, L_{w_n}\} \cap L_s = \{0\},$$

The first requirement for the independent set  $W$  is satisfied.

To verify the second condition, for each  $\ell \in \{1, 2, \dots, d\}$ , the sum of the  $\ell$ -th generating vector of  $L_{v_{i,j}}$  and  $L_{w_j}$  gives the  $\ell$ -th generating element of  $L_s$ . For example, when  $\ell = 1$

$$\begin{aligned}
& \left\{ (10 \dots 0)^{k(j-1)} \oplus (00 \dots 0)^k \oplus (10 \dots 0)^{k(n-j)+1} \right\} \\
& + \left\{ (00 \dots 0)^{k(j-1)} \oplus (10 \dots 0)^k \oplus (00 \dots 0)^{k(n-j)+1} \right\} \\
& = (1000 \dots 0)^{kn+1}.
\end{aligned}$$

This implies that the linear span of  $L_{v_{i,j}}$  and  $L_{w_j}$  contains  $L_s$  as required.

Observe that the first  $d$  generating vectors in  $L_{v_{i,j}}$  have all 0 in the  $(k(j-1)+1)$ -th to the  $(kj)$ -th groups, and the other  $d$  generating vectors in  $L_{v_{i,j}}$  have all 0 in the  $(k(j-1)+i)$ -th group. Hence the linear span of  $L_{v_{i,j}}$  and all other  $L_{w_m}$ 's with  $j \neq m$  has all zero coordinates in this group and therefore contains only the zero element from  $L_s$ .

In order to have the last condition satisfied, subtracting the  $d+1$  generating vector of  $L_{v_{s,r}}$  from the  $d+1$  generating vector of  $L_{v_{i,j}}$  with  $(i,j) \neq (s,r)$  gives

$$\begin{aligned}
& \left[ \bigoplus_{m=1}^{kn} (\lambda_{k(j-1)+i,m} 00 \cdots 0) \right] \oplus (\lambda_{k(j-1)+i} 00 \cdots 0) \\
& - \left[ \bigoplus_{m=1}^{kn} (\lambda_{k(r-1)+s,m} 00 \cdots 0) \right] \oplus (\lambda_{k(r-1)+s} 00 \cdots 0) \\
& = (\lambda_{k(j-1)+i, k(r-1)+s} 00 \cdots 0)^{kn+1} \\
& = \lambda_{k(j-1)+i, k(r-1)+s} (100 \cdots 0)^{kn+1}
\end{aligned}$$

The linear span of this vector contains the first generating vector of  $L_s$ . Since each generating vector of  $L_s$  can be obtained in the same way, the last condition holds as well.

With  $\dim(L_{v_s}) = d$ ,  $\dim(L_{w_j}) = d$  and  $\dim(L_{v_{i,j}}) = 2d$ , we also know that the perfect secret sharing scheme we have constructed has information ratio 2.  $\square$

By Theorem 3.1. and Theorem 3.4. we have the following corollary.

**Corollary 3.5.**

$$2 - 2^{-n+1} \leq R(G'_{k,n}) \leq 2.$$

### 3.3 A Construction of Perfect Secret Sharing Scheme on $G''_{k,n}$

Recall that in the graph  $G''_{k,n}$  defined at the beginning of this chapter, there is no edge between the vertices from different  $V_i$ 's.

**Construction 3.6.** Let  $\lambda_1, \lambda_2, \dots, \lambda_{km}$  be  $km$  distinct integers. For convenience, let  $\lambda_x - \lambda_y$  be denoted by  $\lambda_{x,y}$  and

$$a_{i,j,m} = \begin{cases} \lambda_{k(j-1)+i} & , \text{ where } m = k(t-1) + i \text{ for } t = 1 \cdots n \\ \lambda_{k(j-1)+i,m} & , \text{ otherwise.} \end{cases}$$

Assign to  $L_s$  the subspace spanned by the following  $d$  vectors:

$$(1000 \cdots 0)^{kn+1}, (0100 \cdots 0)^{kn+1}, (0010 \cdots 0)^{kn+1}, \dots, (000 \cdots 01)^{kn+1}.$$

Assign to  $L_{w_j}$  the subspace spanned by the following  $d$  vectors:

$$\begin{aligned} & (0 \cdots 0)^{k(j-1)} \oplus (100 \cdots 0)^k \oplus (0 \cdots 0)^{k(n-j)+1}, \\ & (0 \cdots 0)^{k(j-1)} \oplus (010 \cdots 0)^k \oplus (0 \cdots 0)^{k(n-j)+1}, \\ & \vdots \\ & (0 \cdots 0)^{k(j-1)} \oplus (00 \cdots 01)^k \oplus (0 \cdots 0)^{k(n-j)+1}. \end{aligned}$$

In addition,  $L_{v_{i,j}}$  is assigned the subspace spanned by the following  $2d$  vectors:

$$\begin{aligned} & (100 \cdots 0)^{k(j-1)} \oplus (00 \cdots 0)^k \oplus (100 \cdots 0)^{k(n-j)+1}, \\ & (010 \cdots 0)^{k(j-1)} \oplus (00 \cdots 0)^k \oplus (010 \cdots 0)^{k(n-j)+1}, \\ & \vdots \\ & (00 \cdots 01)^{k(j-1)} \oplus (00 \cdots 0)^k \oplus (00 \cdots 01)^{k(n-j)+1}, \end{aligned}$$





$$\begin{aligned}
L_{w_1,1} = \text{Span}\{ & (000000100100100), (000000010010010), (000000001001001), \\
& (a_{1,1,1}00a_{1,1,2}00a_{1,1,3}00a_{1,1,4}00\lambda_100), \\
& (0a_{1,1,1}00a_{1,1,2}00a_{1,1,3}00a_{1,1,4}00\lambda_10), \\
& (00a_{1,1,1}00a_{1,1,2}00a_{1,1,3}00a_{1,1,4}00\lambda_1)\}
\end{aligned}$$

$$\begin{aligned}
L_{w_2,1} = \text{Span}\{ & (000000100100100), (000000010010010), (000000001001001), \\
& (a_{2,1,1}00a_{2,1,2}00a_{2,1,3}00a_{2,1,4}00\lambda_200), \\
& (0a_{2,1,1}00a_{2,1,2}00a_{2,1,3}00a_{2,1,4}00\lambda_20), \\
& (00a_{2,1,1}00a_{2,1,2}00a_{2,1,3}00a_{2,1,4}00\lambda_2)\}
\end{aligned}$$

$$\begin{aligned}
L_{w_1,2} = \text{Span}\{ & (100100000000100), (010010000000010), (001001000000001), \\
& (a_{1,2,1}00a_{1,2,2}00a_{1,2,3}00a_{1,2,4}00\lambda_300), \\
& (0a_{1,2,1}00a_{1,2,2}00a_{1,2,3}00a_{1,2,4}00\lambda_30), \\
& (00a_{1,2,1}00a_{1,2,2}00a_{1,2,3}00a_{1,2,4}00\lambda_3)\}
\end{aligned}$$

$$\begin{aligned}
L_{w_2,2} = \text{Span}\{ & (100100000000100), (010010000000010), (001001000000001), \\
& (a_{2,2,1}00a_{2,2,2}00a_{2,2,3}00a_{2,2,4}00\lambda_400), \\
& (0a_{2,2,1}00a_{2,2,2}00a_{2,2,3}00a_{2,2,4}00\lambda_40), \\
& (00a_{2,2,1}00a_{2,2,2}00a_{2,2,3}00a_{2,2,4}00\lambda_4)\}
\end{aligned}$$

**Theorem 3.8.** *Construction 3.6. defines a perfect secret sharing scheme on  $G''_{k,n}$  with information 2.*

**Proof.** To show that Construction 3.6. is a perfect secret sharing scheme on  $G''_{k,n}$ , we need to check the following condition.

1. the span of  $L_{w_1}, L_{w_2}, \dots, L_{w_n}$  is trivial,

2. the span of  $L_{v_{i,j}}$  and  $L_{w_j}$  must contain  $L_s$ ,
3. the span of  $L_{v_{i,j}}$  and  $\{L_{w_m} : m \neq j\}$  intersects  $L_s$  in  $\{0\}$ ,
4. the span of two different  $L_v$  and  $L_u$ , where  $v, u \in V_i$ , should contains  $L_s$ , and
5. the span of two different  $L_v$  and  $L_u$ , where  $v \in V_i$  and  $u \in V_j$  with  $i \neq j$ , should be the trivial space  $\{0\}$ .

Note that Construction 3.6. is very similar to Construction 3.2, the only difference lies in the last  $d$  generating vectors of each  $L_{v_{i,j}}$  for  $1 \leq i \leq k$  and  $1 \leq j \leq n$ . Hence the first, second, and third conditions hold by the proof of Theorem 3.4.

To verify that the fourth condition holds as well, we observe that

$$\begin{aligned}
& \left\{ \left[ \bigoplus_{m=1}^{kn} (a_{i,j,m} 00 \cdots 0) \right] \oplus (\lambda_{k(j-1)+i} 00 \cdots 0) \right\} \\
& - \left\{ \left[ \bigoplus_{m=1}^{kn} (a_{i,r,m} 00 \cdots 0) \right] \oplus (\lambda_{k(r-1)+i} 00 \cdots 0) \right\} \\
& = (\lambda_{k(j-1)+i, k(r-1)+i} 00 \cdots 0)^{kn+1} \\
& = (\lambda_{k(j-1)+i, k(r-1)+i}) (100 \cdots 0)^{kn+1}
\end{aligned}$$

The first generating vector of  $L_s$  can be obtained from the  $(d+1)$ -th generating vectors of  $L_{v_{i,j}}$  and  $L_{v_{i,r}}$  with  $j \neq r$ . The linear span of  $L_{v_{i,j}}$  and  $L_{v_{i,r}}$  contains the generating vectors of  $L_s$ , hence the fourth condition is also satisfied. To check the fifth condition, one can easily verify that any generating vector of  $L_s$  cannot be generated by the vectors in any two different vector subspaces  $L_{v_{i,j}}$  and  $L_{v_{s,r}}$  with  $s \neq i$ .

In this construction,  $L_{v_{i,j}}$  is generated by  $2d$  linearly independent vectors,  $L_{w_j}$  and  $L_s$  are both generated by  $d$  linearly independent vectors, thus  $\dim(L_{v_{i,j}}) = 2d$  and  $\dim(L_{w_j}) = \dim(L_s) = d$ . This shows that the information ratio of Construction 3.6. is also 2.

□

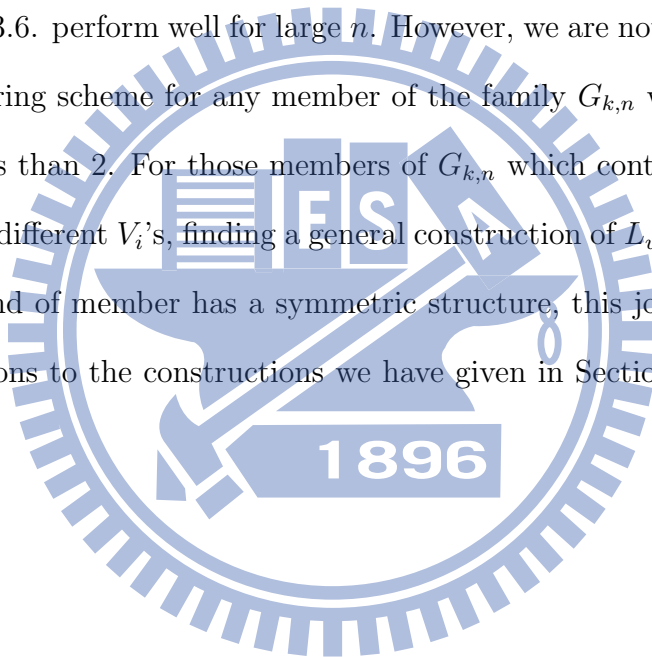
By Theorem 3.1. and Theorem 3.8. we have the following corollary.

**Corollary 3.9.**

$$2 - 2^{-n+1} \leq R(G''_{k,n}) \leq 2.$$

### 3.4 Concluding Remark

The lower bound of the information ratio in Corollary 3.5. and Corollary 3.9. are very close to the upper bound when  $n$  is sufficiently large. Hence Construction 3.2. and Construction 3.6. perform well for large  $n$ . However, we are not sure that if there exists a secret sharing scheme for any member of the family  $G_{k,n}$  whose information ratio is strictly less than 2. For those members of  $G_{k,n}$  which contain some, but not all, edges between different  $V_i$ 's, finding a general construction of  $L_{v_i,j}$  is very difficult. However if this kind of member has a symmetric structure, this job can be done by making modifications to the constructions we have given in Section 3.2 and Section 3.3.



# Bibliography

- [1] C. Blundo, A. De Santis, D. R. Stinson and U. Vaccaro, Graph decompositions and secret sharing schemes, *J. Cryptology*, 8 (1995), pp 39-64.
- [2] E. F. Brickell and D. M. Davenport, On the classification of ideal secret sharing schemes, *J. Cryptology*, 4 (1991), pp 123-134
- [3] E. F. Brickell and D. R. Stinson, Some improved bounds on the information rate of perfect secret sharing schemes, *J. Cryptology*, 5 (1992), pp 153-166.
- [4] L. Csirmaz: Secret sharing on infinite graphs, *Studia Mathematica Hungarica*, vol 44(2007) pp. 297-306 - available as IACR preprint <http://eprint.iacr.org/2005/059>.
- [5] L. Csirmaz: Secret sharing schemes on graphs, *Tatra Mt. Math. Publ* 41 (2008) pp 1-18.
- [6] L. Csirmaz, An impossibility result on graph secret sharing, *Designs, Codes and Cryptography*, 53 (2009), pp 195-209.
- [7] L. Csirmaz and P. Ligeti, On an infinite families of graphs with information ratio  $2 - \frac{1}{k}$ , *Computing*, 85 (2009), pp 127-136.
- [8] L. Csirmaz and G. Tardas, Exact bounds on tree based secret sharing schemes, *Tatracrypt 2007*, Slovakia

- [9] I. Csiszár and J. Körner: Information Theory. Coding Theorems for Discrete Memoryless Systems, Academic Press, New York, 1981.
- [10] F. Matus: Adhesivity of polymatroids, Discrete Mathematics, Vol 307(2007) 21, pp 2464-2477.
- [11] D. R. Stinson, Decomposition constructions for secret sharing schemes, IEEE Transactions on Information Theory, 40 (1994), pp 118-125.
- [12] M. van Dijk, On the information rate of perfect secret sharing schemes, Designs, Codes and Cryptography, 6 (1995), pp 143-169.
- [13] M. van Dijk, T. Kevenaar, G. Schrijen, P. Tuyls: Improved constructions of secret sharing schemes by applying  $(\lambda, \omega)$ -decompositions, Inf. Process. Lett. vol 99(4), 2006, pp.154-157.
- [14] Z. Zhang, R. W. Yeung: On characterization of entropy function via information inequalities, IEEE Trans. Inform.Theory Vol 44, 1998, pp 1440-1452.