Information Rates for Secret Sharing over Various Access Structures

by

Jessica Ruth Metcalf-Burton

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in The University of Michigan
2009

Doctoral Committee:

Professor Andreas R. Blass, Chair
Professor Daniel M. Burns Jr.
Professor Melvin Hochster
Associate Professor Kevin J. Compton
Associate Professor Anna C. Gilbert

ACKNOWLEDGEMENTS

This dissertation, like most, is the end result of many years of work and goofing off, and as such owes its existence to a great number of people.

Thanks to my committee: Andreas Blass, Daniel Burns, Kevin Compton, Anna Gilbert, and Mel Hochster, for letting me graduate. A little extra thanks to ABlass for the handwaving and colored chalk, and to Mel for distracting me with crossword puzzles during teatime.

Thanks to the many math teachers I've had throughout the years: Steve Waldhorn for getting me really interested in math in fifth grade, Victor Stekoll for that final exam on which I beat all the boys, Mr. Donaldson for combining math and poetry, Mr. Walstein for taking us to ARML in high school, and Professor Kueker for that first logic class in college. Thanks also to the late Juha Heinonen, whose amazing teaching and wonderful personality almost converted me from a logician to an analyst.

Thanks to some non-math teachers: Phil Resnik for involving me in a research project in college, Meesh for the unconditional love and support, Sandy Mack for the sermons, and Bradford Gowen for giving me a place where I could think about music instead.

Thanks to Carles Padró for being the first mathematician outside the University of Michigan to take an interest in my dissertation work. Thanks to Randy and Steve for helping me sort rocks by color while blindfolded, and thanks to Chris for the first

summer at “Papa John’s.”

Thanks to my friends, for alternately encouraging me and distracting me as appropriate: Mariah Branch, Zeynep Dilli, Ashley Eden, Aaron Elkiss, Hester Graves, Chad Groft, Jeffrey Huo, Benjamin Kleber, Lisa Pearl, Marie Snipes, Nicole Travers, Benjamin Weiss, and Kevin Wildrick.

Thanks to Zachary Williams for the tea and kisses, and thanks to Mike Anglin and Kathy Clark, my honorary Ann Arbor family.

Finally, thanks to my family, for being there throughout it all: Mom, Dad, Justin, Jules, and Jonathan.

TABLE OF CONTENTS

LIST OF FIGURES

Figure

LIST OF TABLES

Table

CHAPTER 1

Introduction

Secret sharing schemes were first introduced independently by Shamir [25] and Blakley [2] as a means of protecting cryptographic keys. In a secret sharing scheme, a dealer hands out pieces of a secret to each member of a group of participants, so that (1) any set of participants that is supposed to be qualified to determine the secret can actually determine the secret, and (2) any other set of participants learns nothing about the secret. The collection of qualified sets is called an access structure. The formal definition of secret sharing uses the Shannon entropy function [14], where the entropy of a random variable X may be thought of as the amount of information contained in X.

One way of measuring the efficiency of a secret sharing scheme is via the information rate, which compares the size of the secret to the size of a participant's share. The information rate of an access structure is the supremum of the information rate over all schemes for that access structure.

There are many open problems in secret sharing regarding the information rates of certain access structures and classes of access structures. The general technique for finding information rates is to bound the rates from above and below. To show a lower bound on the rate of an access structure, it is enough to find a scheme for

the structure realizing that bound. Proofs of upper bounds usually involve adding large collections of information inequalities, which are any inequalities that must be satisfied by the entropy function.

This work is organized into four chapters. In Chapter 2 we introduce the background and context needed to state our results. We recall some basic probability so that we can define Shannon entropy. We use Shannon entropy to present a formal definition of secret sharing and some basic ideas surrounding secret sharing that will be needed in the remainder of the work. We examine connections between matroids and secret sharing schemes, and introduce linear random variables and linear secret sharing schemes.

In Chapter 3 we discuss basic and non-Shannon information inequalities. We introduce a method for creating visual representations of Shannon inequalities. The visual representations are helpful for adding large collections of Shannon inequalities, and also for determining which inequalities should be added together in particular situations. We use these visual representations to give a pictorial proof of Ingleton's Inequality on four linear random variables, and then prove that Ingleton's Inequality holds if we replace the linearity assumption with certain independence assumptions. The vailidity of Ingleton's Inequality under these new hypotheses leads to a new proof of the Zhang-Yeung inequality. We present the known 4-variable non-Shannon inequalities in a format that allows the reader to see some of the similarities in their structures.

In Chapter 4 we give new results on the information rates of the access structures induced by the Vámos matroid, which is of interest for several reasons. Since any matroid on fewer than eight points is representable and the Vámos matroid is not [20], the Vámos matroid is a minimal example of a non-representable matroid. It is known

that ideal access structures must be induced by matroids, that representable matroids induce ideal access structures [6], and that access structures with information rate greater than 2/3 are also induced by matroids [19]. However, little is known about the information rates of non-representable matroids. The Vámos matroid is the first known example of a matroid whose induced access structures do not admit ideal schemes [23]. The Vámos matroid provides the first known example of a matroid whose induced access structures have rates bounded away from 1, and also the first examples of access structures with rates strictly between 2/3 and 1 [1, 19].

The exact information rates of V_1 and V_6 are unknown. Martí-Farré and Padró showed that the rates must be at least 3/4 [19], while Beimel, Livne, and Padró used the Zhang-Yeung inequality to show that the information rates of V_1 and V_6 have upper bounds of 10/11 and 9/10 respectively [1]. Here we improve the best known upper bounds on the information rates of V_1 and V_6 from 10/11 to 8/9 and from 9/10 to 17/19 respectively. The method we introduce to obtain the bound for V6 can be applied to all other 4-variable non-Shannon information inequalities of which we are aware.

Finally, in Chapter 5 we consider an infinite sequence of non-matroid-induced access structures called the "king and n pawns" structures. Along with 3 other access structures whose information rates are known to be 2/3 [27], the king and n pawns structures for $n \geq 3$ are the non-matroid-induced access structures minimal under the operations of deletion and contraction as defined for access structures. We show that the information rate of the king and n pawns structure is $\frac{n-1}{2n-3}$. To do this we prove the upper bound using sums of information inequalities found using visual representations, and prove the lower bound by exhibiting a secret sharing scheme with rate $\frac{n-1}{2n-3}$.

CHAPTER 2

Preliminaries and Introduction to Secret Sharing

2.1 Introduction

In the following sections we review some probability theory, define the entropy function, and provide a formal introduction to secret sharing. We discuss one way to measure the efficiency of a secret sharing scheme, and mention connections between matroids and secret sharing schemes. We also introduce linear random variables and linear secret sharing.

Throughout we use the notational conventions that $\mathbb{R}^+$ denotes the set of non-negative reals, and that for sets X, Y we abbreviate $X \cup Y$ by XY.

2.2 Probability

In order to talk precisely about the notion of information in secret sharing, we require some finite probability theory. A formal introduction may be found in [10]; less formal definitions may be found in many books dealing with cryptography or information theory, for example [29]. For the rest of this work we assume the reader is familiar with the material in this section.

Definition 2.1. A *finite probability space* is a finite set Ξ with an associated function p from Ξ to the non-negative reals such that

(1) $p(\xi) \geq 0$ for all $\xi \in \Xi$, and

(2) $\sum_{\xi \in \Xi} p(\xi) = 1$.

A function p on Ξ satisfying (1) and (2) is called a *probability distribution function*.

A finite probability space may be thought of as a table listing all possible outcomes of an experiment, along with the likelihood of each possible outcome.

Definition 2.2. We say a probability distribution function p on Ξ is *uniform* if for all $\xi \in \Xi$, $p(\xi) = \frac{1}{|\Xi|}$, that is, p gives equal weight to each possible outcome. When we choose an element of a set according to a uniform probability distribution we say we are choosing an element *uniformly at random*.

An example of a uniform probability distribution arises when we flip a fair coin. The probability space in this situation is the set $\{\text{heads}, \text{tails}\}$ with the constant function $p : \{\text{heads}, \text{tails}\} \to \{1/2\}$.

Definition 2.3. A *finite random variable* X is any function defined on a finite probability space Ξ. Let $\text{range}(X) = X(\Xi)$. For $x \in \text{range}(X)$, the *probability that* $X = x$ is given by

$$p(X = x) = \sum_{\xi : X(\xi) = x} p(\xi).$$

With a slight abuse of terminology, we call this p the probability distribution on the random variable X. When the random variable being used is clear from context we will write $p(x)$ as an abbreviation for $p(X = x)$.

Henceforth we will omit the word "finite" when introducing random variables and probability spaces, as these are the only types of random variables and probability spaces we will use.

Remark 2.4. For a fixed probability space Ξ and random variables $X_1, \ldots, X_n$ on Ξ, the tuple $X = (X_1, \ldots, X_n)$ is also a random variable, with the function X on Ξ sending the element $\xi \in \Xi$ to the tuple $(X_1(\xi), \ldots, X_n(\xi))$. Thus in any statement that mentions a single random variable X, we may also take X to be a tuple of random variables. Notice that the order in which we write $X_1, \ldots, X_n$ is unimportant in practice, since changing the order will not affect the probability that $X_1 = x_1, \ldots, X_n = x_n$ simultaneously. When making a statement involving multiple random variables, we assume the random variables are defined on the same probability space.

Definition 2.5. The *joint probability distribution* of the random variables $X_1, \ldots, X_n$ is given by the probability distribution on the random variable $(X_1, \ldots, X_n)$. For each individual random variable X_i there is an induced probability distribution function, where the probability that $X_i = x$ is given by

$$p(X_i = x) = \sum_{x_1, \ldots, x_n} p(X_1 = x_1, \ldots, X_n = x_n)$$

where $x_i = x$ and the other variables range over all

$$x_1 \in \text{range}(X_1), \ldots, x_{i-1} \in \text{range}(X_{i-1}), x_{i+1} \in \text{range}(X_{i+1}), \ldots, x_n \in \text{range}(X_n).$$

Definition 2.6. For random variables X and Y, let $x \in \text{range}(X)$ and $y \in \text{range}(Y)$. The *conditional probability that $X = x$ given that $Y = y$* is defined by

$$p(X = x | Y = y) = \frac{p(X = x, Y = y)}{p(Y = y)}.$$

Definition 2.7. If $p(X = x, Y = y) = p(X = x)p(Y = y)$ for all $x \in \text{range}(X)$ and $y \in \text{range}(Y)$, we say that X and Y are *independent.* If X and Y are not independent we say that they are *dependent.*

An equivalent definition of independence is that for all $x \in \text{range}(X)$ and $y \in \text{range}(Y)$, $p(X = x|Y = y) = p(X = x)$. Intuitively, X and Y are independent if knowing the value of one tells you nothing about the value of the other.

Example 2.8. Suppose we have two dice, D1 and D2, which we roll individiually. Let X be the face showing on D1 and Y the face showing on D2. Then X and Y are independent, because knowing the value of D2 tells you nothing about the value of D1, and vice versa.

Example 2.9. Now take three dice D1, D2, and D3, and roll them each once. Let X be the faces showing on D1 and D3, Y the faces showing on D2 and D3, and Z the face showing on D3. Then X and Y are dependent, as they must show the same face for D3. However, once we know the value of Z the remaining pieces of X and Y are independent, since the values of D1 and D2 are still independent of each other.

This example suggests the existence of another type of independence.

Definition 2.10. For random variables X, Y, Z we say that X *and* Y *are conditionally independent given* Z if for all $x \in \text{range}(X)$, $y \in \text{range}(Y)$, and $z \in \text{range}(Z)$,

$$p(X = x|Z = z)p(Y = y|Z = z) = p(X = x, Y = y|Z = z).$$

In Example 2.9 X and Y are conditionally independent given Z.

2.3 Shannon Entropy and Mutual Information

Suppose a friend is going to send you one of two messages, chosen uniformly at random. One message is the string of bits 11110 and the other is the string of bits 11111. When you receive a message you will have to read 5 bits before you know which message you have received, since the only difference between the messages is the last bit. The possible messages could just as well have been 0 and 1. Intuitively,

upon receiving one of two equally likely messages, you will really have learned only one bit worth of information.

Now suppose there are four possible messages, each with equal probability: 00, 01, 10, and 11. In this case you do need to read both bits to know what the message is, as there is no way to convey four different messages with only one bit.

To complicate the situation further, we allow non-uniform probabilities. Suppose there are three possible messages: $0, 10$, and 11, with probabilities $1/2, 1/4$, and $1/4$ respectively [29]. Half the time your friend can send just the single bit 0. The other half of the time your friend will choose between 10 and 11, each of these times sending you two bits of information. On average, the number of bits necessary to send the message is

$$\frac{1}{2}(1) + \frac{1}{4}(2) + \frac{1}{4}(2) = \frac{3}{2}.$$

This is in fact the best average message length possible with the given probabilities. We call this value the entropy of the message.

Definition 2.11 ([26])**.** Let X be a random variable with range $\{x_1, \ldots, x_n\}$, and probability $p(x_i)$ that $X = x_i$. The *Shannon entropy* of X is defined by

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log p(x_i)$$

where by convention $0 \log 0 = 0$.

The logarithm in the definition of Shannon entropy may use any base, depending on whether we want to measure information in bits (base 2), digits (base 10), nats (base e), or something else. We will usually think of the logarithms as base 2 and the information as being measured in bits.

Lemma 2.12. *Suppose X is a random variable with $|range(X)| = n$ and the uniform probability distribution, so that $p(x) = 1/n$ for all $x \in X$. Then $H(X) = \log n$.*

Proof.

$$H(X) = -\sum_{i=1}^{n} \frac{1}{n} \log \frac{1}{n} = -\log \frac{1}{n} = \log n. \qquad \square$$

Shannon entropy may be thought of as the average amount of information required to transmit the value of a random variable, or as as the average amount of information one gains by learning the value of a random variable. Since the logarithms in Definition 2.11 are non-positive and probabilities are always non-negative, we have the following lemma:

Lemma 2.13. $0 \leq H(X)$.

This makes intuitive sense: one cannot use a negative number of bits to transmit a message, and neither should learning the content of a message decrease the amount of information to which one has access.

Definition 2.14 (Joint Entropy)**.** If random variables $X_1, \ldots, X_k$ on the same probability space take values in $\text{range}(X_1), \ldots, \text{range}(X_k)$, respectively, the *joint entropy of* $X_1, \ldots, X_k$ is the entropy of the random variable $(X_1, \ldots, X_k)$. The joint entropy may also be written as

$$H(X_1, \ldots, X_k) = -\sum_{x_1, \ldots, x_k} p(x_1, \ldots, x_k) \log p(x_1, \ldots, x_k).$$

where the sum is taken over all $x_1 \in \text{range}(X_1), \ldots x_k \in \text{range}(X_k)$.

Definition 2.15 (Conditional Entropy)**.** For random variables X and Y with respective domains $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_m\}$, the *conditional entropy of* Y *given* X is

$$H(Y|X) = -\sum_{i=1}^{n} \sum_{j=1}^{m} p(x_i, y_j) \log p(y_j|x_i).$$

An equivalent definition is given by the identity

$$H(Y|X) = H(X, Y) - H(X). \tag{2.1}$$

A proof of the equivalence may be found in [22, p. 95], or worked out directly from the definitions and the fact that $p(x_i) = \sum_{j=1}^{m} p(x_i, y_j)$.

Since the logarithms in the definition are non-positive and the probabilities are non-negative, conditional entropy is also non-negative.

Lemma 2.16. $0 \leq H(Y|X)$.

We will refer to Shannon entropy, conditional entropy, and joint entropy collectively as *entropy*, relying on context and notation to clarify the particular type of entropy to which we refer.

Using the definition of joint entropy, we generalize the definition of the entropy function to allow as input a set of random variables [11].

Definition 2.17. For a set $X = \{X_1, \ldots, X_n\}$ of random variables, let

$$H(X) = H(X_1, \ldots, X_n).$$

By Remark 2.4 this is well-defined.

Recall that for sets X, Y we abbreviate $X \cup Y$ by XY. We may thus use $H(X, Y)$, $H(X \cup Y)$, and $H(XY)$ interchangeably. Given a set Z of random variables on the same sample space, we now consider the *entropy function on* Z to be the map H from 2^Z to non-negative real numbers given by Definition 2.17.

Lemma 2.18 (Monotonicity)**.** *The entropy function on sets of random variables is monotone: For sets X, Y of random variables,*

$$H(X) \leq H(XY).$$

Proof. Since $H(Y|X) \geq 0$,

$$H(X) \leq H(X) + H(Y|X) = H(XY).$$

□

Lemma 2.19. *For sets X, Y of random variables,*

$$H(X|Y) \leq H(X).$$

Proof. While the result is frequently quoted, the proof (due to Gallager [12, 24]) is not, so we include it here. We show $H(X|Y) - H(X) \leq 0$. One may check that by the definitions of conditional entropy and marginal probability,

$$H(X|Y) - H(X) = (\log e) \sum_{x,y} p(x,y) \ln \frac{p(x)}{p(x|y)}.$$

Consider the sum to be only over those terms for which $p(x,y)$ is nonzero, and so also $p(x)$ and $p(x|y)$ are nonzero. As one may check using basic calculus, $\ln z \leq z - 1$ for all $z > 0$. We substitute this into the above summation to get

$$\begin{aligned} H(X|Y) - H(X) \leq & (\log e) \sum_{x,y} p(x,y) \left(\frac{p(x)}{p(x|y)} - 1 \right) \\ = & (\log e) \left(\left(\sum_{x,y} p(x,y) \frac{p(x)}{p(x|y)} \right) - 1 \right). \end{aligned}$$

Since $p(x,y) = p(y)p(x|y)$,

$$\begin{aligned} \sum_{x,y} p(x,y) \frac{p(x)}{p(x|y)} = & \sum_{x,y} p(x)p(y) \\ = & \left(\sum_{x} p(x) \right) \left(\sum_{y} p(y) \right) \\ = & 1. \end{aligned}$$

Thus

$$H(X|Y) - H(X) \leq (\log e)(1 - 1) = 0.$$ □

Lemma 2.20 (Submodularity)**.** *The entropy function on sets of random variables is submodular: for sets X, Y, Z of random variables,*

$$H(Z) + H(XYZ) \leq H(XZ) + H(YZ).$$

Equivalently,

$$H(X|YZ) \leq H(X|Z).$$

Proof. One can prove $H(X|YZ) - H(X|Z) \leq 0$ with the method used in the proof of Lemma 2.19 [12]. □

Sometimes it will be convenient to work with other measures of information besides the entropy function. Useful references are [12, 32].

Definition 2.21. For sets X, Y, Z of random variables, the *mutual information of X and Y* is defined by

$$I(X;Y) = H(X) + H(Y) - H(XY)$$

and the *conditional mutual information of X and Y given Z* is defined by

$$I(X;Y|Z) = H(XZ) + H(YZ) - H(Z) - H(XYZ).$$

The next lemma follows from the monotonicity of conditional entropy and the submodularity of the entropy function.

Lemma 2.22. *Mutual information and conditional mutual information are non-negative.*

Intuitively, $I(X;Y)$ is the (average) amount of information X and Y have about each other. By the definition of conditional entropy $I(X;Y) = H(X) - H(X|Y)$. This may be interpreted as the amount of information in X, minus the amount of information X has that Y did not already know. What is left must be the information available to X that was already available to Y.

Using the notions of conditional entropy and mutual information, we can talk about the independence of random variables without explicitly mentioning probabil-

ity. The proof of the next theorem follows from examining the proof of Lemma 2.19 in the case where equality holds.

Theorem 2.23 ([12])**.** *Two random variables X and Y are independent if and only if the following equivalent conditions hold:*

$$I(X;Y) = 0$$

$$H(X) = H(X|Y)$$

$$H(XY) = H(X) + H(Y).$$

Similarly, we can use the notions of entropy and mutual information to talk about conditional independence.

Theorem 2.24 ([12])**.** *Two random variables X and Y are conditionally independent given Z if and only if the following equivalent conditions hold:*

$$I(X;Y|Z) = 0$$

$$H(Z) + H(XYZ) = H(XZ) + H(YZ).$$

Since the second equation in the theorem above is the submodularity of the entropy function with equality instead of inequality, we make the following definition.

Definition 2.25. If $I(X;Y|Z) = 0$, or equivalently if X and Y are conditionally independent given Z, we say the entropy function is *modular for X and Y given Z.*

2.4 Secret Sharing Schemes

Let P be a finite set of participants, among whom we would like to share a secret. Only specified sets of participants are qualified to know the secret.

Definition 2.26. An *access structure* Γ on P is an upward-closed collection of subsets of P such that $\emptyset \notin \Gamma$. Sets $X \subseteq P$ are called *qualified* if they belong to Γ and

unqualified otherwise. Since Γ must be upward closed, it is fully determined by its *minimal qualified subsets*, which are those qualified sets for which no proper subset is qualified.

Without loss of generality, we assume that each participant in P belongs to some minimal qualified subset. Otherwise we can delete that participant from the set P without affecting the minimal qualified sets of the access structure.

Example 2.27. Suppose there are three people p_1, p_2, p_3 such that any two are qualified, but no individual is qualified. The access structure for this situation is $\Gamma = \{\{p_1, p_2\}, \{p_1, p_3\}, \{p_2, p_3\}, \{p_1, p_2, p_3\}\}$. The minimal qualified subsets of Γ are $\{p_1, p_2\}, \{p_1, p_3\}, \{p_2, p_3\}$.

We think of the secret as belonging to a special participant called the *dealer*, who is not included in P. Intuitively, a secret sharing scheme for Γ is a way for the dealer to use the value of the secret and some randomly generated information to deal out one or more *shares* to each of the other participants in such a way that qualified sets are able to reconstruct the secret by combining their shares, while unqualified sets cannot learn any information about the secret.

Definition 2.28 ([14])**.** Fix an access structure Γ. Let Σ be a collection of random variables consisting of one random variable S for the secret and, for each participant $x \in P$, a random variable for the share belonging to x. We use $H(x)$ to denote the Shannon entropy of the random variable corresponding to x, and for any nonempty subset $X \subseteq P \cup \{S\}$, we use $H(X)$ to denote the entropy of the corresponding set of random variables. We call Σ a *(perfect[1]) secret sharing scheme for* Γ if it has the

[1] "Perfect" refers to the third condition of our definition. Some authors consider more general secret sharing schemes in which unqualified sets of participants may learn a nonzero amount of information about the secret [3], or in which unqualified sets with reasonable computational resources obtain no information about the secret [21]. Henceforth we consider only perfect secret sharing schemes, and therefore omit the word "perfect."

following properties:

- $H(S) > 0$ to ensure there is a secret to share.
- If $X \in \Gamma$ then $H(S|X) = 0$, that is, the participants in X are able to combine their shares to completely determine the value of the secret.
- If $X \notin \Gamma$ then $H(S|X) = H(S)$, that is, the uncertainty about the secret does not change even when all participants in X pool their shares.

The probability space of the random variables in Σ includes all possible ways to choose a secret and suitable random information. We assume the probability distribution on the random variable corresponding to the secret is uniform, since by [4] this distribution is independent of the entropies of unqualified sets of participants.

Remark 2.29. With a slight abuse of notation, one may consider the dealer to be a special participant in the access structure who is individually qualified to reconstruct the secret. This requires adjoining S to the set of participants P, and adjoining to Γ the minimal qualified set $\{S\}$ and all its supersets. All sets adjoined to Γ will satisfy $H(S|X) = 0$, and the values $H(S|X)$ for sets X in the original Γ will be unaffected.

Example 2.30 ([25])**.** Let $P = \{p_1, p_2, p_3\}$ and let $\Gamma = \{\{p_1, p_2\}, \{p_1, p_3\}, \{p_2, p_3\}, \{p_1, p_2, p_3\}\}$ as in Example 2.27. Consider a finite field K of size k where k is a prime greater than 3. For a given secret $s \in K$, the dealer picks uniformly at random a constant $a \in K$, constructs the function $f(x) = ax + s$, and gives to participant p_i the value $f(i)$. The condition $k > 3$ ensures that no participant will have a share identical to the secret. Qualified sets can determine the secret, since two distinct points on a line determine the y-intercept of that line. Unqualified sets gain no information about the secret: for any possible secret and any share $f(i)$, there is exactly one

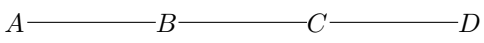


Figure 2.1: The 4-Person Path

A	B	C	D
r	$r \oplus s$	r	
		t	$t \oplus s$

Table 2.1: Scheme to Share 1 Bit Over the 4-Person Path

line through the points $(0, s)$ and $(i, f(i))$. Thus to an individual participant any y-intercept will appear equally likely.

Example 2.31. Consider the set of participants $\{A, B, C, D\}$ and the access structure Γ whose minimal qualified subsets are $\{A, B\}, \{B, C\}, \{C, D\}$. Γ may be visualized as a four-person "path," as shown in Figure 2.1, where two participants are qualified if there is an edge between them. We present two secret sharing schemes for this access structure.

1. To share a single bit $s \in \{0, 1\}$ over Γ, the dealer chooses uniformly at random a pair of bits r and t. The dealer then hands out shares to the other participants as shown in Table 2.1, where $\oplus$ is addition modulo 2. This is indeed a secret sharing scheme: any two adjacent participants can indeed recover the value s, while for two non-adjacent participants any value of the secret will appear equally likely.

2. To share two bits $s, s' \in \{0, 1\}$ over Γ, the dealer chooses uniformly at random four bits r, r', t, t', and hands out shares according to Table 2.2. Again, this is a secret sharing scheme, as two adjacent participants can determine both s and s', but two non-adjacent participants will consider any value of the secret equally likely.

A	B	C	D
r	$r \oplus s$	r	
		t	$t \oplus s$
	t'	$t' \oplus s'$	t'
$r' \oplus s'$	r'		

Table 2.2: Scheme to Share 2 Bits Over the 4-Person Path

2.5 Information Rate

The efficiency of a secret sharing scheme can be measured in terms of information rate, a value which indicates the size of participants' shares relative to the size of the secret. The largest share size handed out by the dealer will determine the efficiency of the overall scheme.

Definition 2.32. Given a secret sharing scheme Σ and a participant $x \in P$, the *information rate of* x is defined by

$$\rho(x) = \frac{H(S)}{H(x)}.$$

The information rate of the secret sharing scheme Σ is defined by

$$\rho(\Sigma) = \min_{x \in P} \rho(x).$$

The information rate of a secret sharing scheme will always be between zero and one [7, 8]. Higher information rates are considered better, since we would like shares to be as small as possible in practice.

Definition 2.33. A secret sharing scheme with information rate 1 is said to be *ideal*.

Intuitively, the efficiency of an access structure is given by the best information rate of secret sharing scheme possible for that access structure. However, there may not be a best secret sharing scheme, so we define the information rate of an access structure as a limit.

Definition 2.34. The information rate of an access structure Γ, $\rho(\Gamma)$, is the supremum of $\rho(\Sigma)$ over all Σ that are secret sharing schemes for Γ. An access structure for which there exists an ideal secret sharing scheme is called *ideal*, and an access structure whose information rate equals one is said to be *nearly ideal*.

Example 2.35. The secret sharing scheme given in Example 2.30 is ideal, and hence the access structure is also ideal.

Example 2.36. Let Γ be the access structure given in Example 2.31. We saw two different schemes for this Γ, the first with rate $1/2$ and the second with rate $2/3$. It turns out that $2/3$ is the highest information rate possible for this access structure [27], and so $\rho(\Gamma) = 2/3$.

2.6 Minors of Access Structures

Given an access structure Γ on a set P of participants and a subset $Z \subseteq P$, there are two ways, introduced in [24], that we can remove the participants in Z to obtain an access structure Γ' on $P \setminus Z$. One way is to take for Γ' those sets that were qualified without any help from participants in Z.

Definition 2.37. If we *delete* the participants in Z, we obtain the access structure

$$\Gamma' = \{X \subseteq P | X \cap Z = \emptyset\}.$$

The other way is to take for Γ' those sets that were indeed qualified with help from the participants in Z.

Definition 2.38. If we *contract* the participants in Z, we obtain the access structure Γ' whose qualified sets are all those of the form $X \setminus Z$ where XZ is qualified in Γ. We only allow contractions where Z is unqualified. Otherwise we will have $\emptyset \in \Gamma'$, in which case Γ' would not actually be an access structure.

The operations of deletion and contraction on access structures commute [24]. That is, if Z_1 and Z_2 are disjoint subsets of P, with Z_2 unqualified, then we obtain the same access structure whether we first delete Z_1 and then contract Z_2, or whether we first contract Z_2 and then delete Z_1.

Definition 2.39. An access structure obtained from Γ by any combination of deletions and contractions is called a *minor* of Γ.

Given any secret sharing scheme Σ for the access structure Γ', the operations of deletion and contraction induce operations on Σ that result in a secret sharing scheme Σ' for Γ'. Deleting the participants in Z corresponds to destroying the shares of those participants in the scheme Σ. Contracting the participants in Z corresponds to publishing their shares, so that every remaining participant can see those shares. Formally, "publishing" involves fixing a tuple of values for the shares of the participants in Z, and adjusting the remaining random variables according to the resulting conditional probability distribution.

Under the scheme Σ', the information rates of participants in $P \setminus Z$ will be the same as they were under Σ. Thus the information rate of Σ' cannot be worse than that of Σ. The information rate of Σ' may be better than that of Σ, since we may be removing participants with poor (low) information rates. This reasoning leads us to the following fact.

Theorem 2.40. *If Γ' is a minor of Γ, $\rho(\Gamma) \leq \rho(\Gamma')$.*

2.7 Normalized Entropy for Secret Sharing Schemes

In order to simplify notation and computations, we introduce a variation of Shannon entropy that lets us assume the entropy of the secret is 1.

Fix a secret sharing scheme Σ. We define the *normalized entropy* of a nonempty set $X \subseteq P$ by

$$h(X) = \frac{H(X)}{H(S)}$$

and the *conditional normalized entropy of X given Y* for nonempty sets $X, Y \subseteq P$ by

$$h(X|Y) = \frac{H(X|Y)}{H(S)}.$$

Since we have assumed that $H(S)$ is strictly positive and since all values of the entropy function H are non-negative, the normalized entropy and conditional normalized entropy are well-defined and non-negative. We observe that the information rate for a participant $x \in P$ is the reciprocal of the normalized entropy for that participant:

$$\rho(x) = \frac{1}{h(x)}. \tag{2.2}$$

Recall that the Shannon entropy function on sets of random variables is monotone and submodular. Dividing through the appropriate inequalities by the positive quantity $H(S)$, we see that the normalized entropy function is also monotone and submodular. Some additional useful facts about h are described in the following lemmas. We assume that X, Y are nonempty subsets of P. Recall that we abbreviate $X \cup Y$ by XY.

Lemma 2.41. *If $X \in \Gamma$ then $h(X) = h(XS)$.*

Proof. From the definitions of secret sharing scheme and conditional entropy, if $X \in \Gamma$ then

$$0 = H(S|X) = H(XS) - H(X).$$

Dividing through by $H(S)$ and rearranging gives the desired result. □

Lemma 2.42. *If* $X \notin \Gamma$ *then* $1 = h(XS) - h(X)$.

Proof. From the definitions of secret sharing scheme and conditional entropy, if $X \notin \Gamma$ then

$$H(S) = H(S|X) = H(XS) - H(X).$$

Dividing through by $H(S)$ gives the desired result. □

Lemma 2.43 (+-Monotonicity)**.** *If* $X \notin \Gamma$ *but* $XY \in \Gamma$ *then* $1 \leq h(XY) - h(X)$.

Proof. By the monotonicity of h and Lemmas 2.41 and 2.42,

$$1 = h(XS) - h(X) \leq h(XYS) - h(X) = h(XY) - h(X).$$ □

Lemma 2.43 says that if X is unqualified and adding the participants in Y produces a qualified set, then the participants in Y must contribute at least 1 to the normalized entropy of X. A slight generalization of this gives the following lemma, which says that if adding the participants in Y to an unqualified superset of X produces a qualified set, then Y must still contribute at least 1 to the normalized entropy of X.

Lemma 2.44 (Generalized +-Monotonicity)**.** *If* $XZ \notin \Gamma$ *but* $XYZ \in \Gamma$ *then* $1 \leq h(XY) - h(X)$.

Proof. By Lemma 2.43

$$1 \leq h(XYZ) - h(XZ)$$

and by the submodularity of h

$$h(X) + h(XYZ) \leq h(XY) + h(XZ).$$

If we add these inequalities, cancel terms, and rearrange, we get the desired result.

□

Note that Lemma 2.43 is the special case of Lemma 2.44 with $Z = \emptyset$.

Lemma 2.45 (+-Submodularity)**.** *If* $Z \notin \Gamma$ *but* $XZ, YZ \in \Gamma$ *then*

$$h(Z) + h(XYZ) + 1 \quad \leq \quad h(XZ) + h(YZ).$$

Proof. By the submodularity of h,

$$h(ZS) + h(XYZS) \quad \leq \quad h(XZS) + h(YZS).$$

Since $XZ, YZ, XYZ \in \Gamma$, adding S to any of these sets does not change their normalized entropy. However, by Lemma 2.42

$$h(ZS) = h(Z) + 1. \qquad \square$$

As we will use the preceeding three lemmas frequently, for the sake of readability we will refer to them by name rather than by number.

2.8 Matroids

A matroid is a combinatorial object that generalizes notions of independence such as independence in a vector space and algebraic independence. We give a brief introduction to matroids, following [20, 30].

Definition 2.46. A *matroid* M on a finite set Q is a collection $\mathfrak{I}$, called the *independent* subsets of Q, such that

- the empty set is independent,
- subsets of independent sets are independent, and
- if X, Y are independent with $|X| = |Y| + 1$ there is $x \in X \setminus Y$ such that $Y \cup \{x\}$ is independent.

Any set that is not independent is called *dependent*. Maximal independent sets are called *bases*, and minimal dependent sets are called *circuits*. The *rank* of a subset X of Q is the size of the largest independent subset of X.

While we gave an axiomatization of matroids in terms of independent sets, matroids can also be axiomatized in other ways, such as in terms of their bases, circuits, or rank function.

Theorem 2.47 ([30])**.** *A function $r : 2^Q \to \mathbb{Z}$ is the rank function of a matroid on Q if and only if for all subsets X, Y of Q*

- $0 \leq r(X) \leq |X|$
- *if $X \subseteq Y$ then $r(X) \leq r(Y)$*
- $r(XY) + r(X \cap Y) \leq r(X) + r(Y)$.

Note that the first condition implies $r(\emptyset) = 0$.

A particularly nice class of matroids are those that can be mapped into vector spaces in such a way as to preserve their independence structure.

Definition 2.48. We say a matroid M over Q is *representable over the field F* if there exists a vector space V over F with a map $f : Q \to V$ such that for any set $X \subseteq Q$, $f(X)$ is independent as a collection of vectors in V if and only if X is an independent set of M.

Given a matroid M on a set Q , there are two natural ways to produce matroids on subsets of Q.

Definition 2.49 (Deletion)**.** If $\mathfrak{I}$ is the set of independent sets of M and $T \subseteq Q$, let $M \backslash T$ be the matroid whose independent sets are

$$\{X : X \subseteq Q \setminus T, X \in \mathfrak{I}\}.$$

We call $M \backslash T$ the *deletion* of T from M.

Definition 2.50 (Contraction)**.** If $\mathfrak{I}$ is the set of independent sets of M and $T \subset Q$, let M/T be the matroid whose independent sets are

$$\{X \subseteq Q \setminus T : \exists Y \text{ a maximal independent subset of } T \text{ s. t. } XY \text{ is independent}\}.$$

We call M/T the *contraction* of T from M.

The operations of deletion and contraction commute.

Definition 2.51. Any matroid obtained from a given matroid M by some combination of deletions and contractions is called a *minor* of M.

2.9 Matroids and Secret Sharing

Given a matroid M over Q, for each element $x \in Q$ there is an *induced access structure* Γ_x over the participants $P = Q \setminus \{x\}$, where x is the dealer [6, 19]. The minimal qualified sets of Γ_x are those subsets $Y \subseteq P$ for which $Y \cup \{x\}$ is a circuit in the matroid M. Intuitively, if $Y \cup \{x\}$ is a circuit then x depends on Y, so it makes sense to think of x as the secret and of Y as a qualified set.

For matroid-induced access structures, the notions of deletion and contraction for matroids and for access structures agree. Let M and Γ_x be as above. If $Z \subseteq P$, then the access structure induced by the matroid $M \backslash Z$ with x as the dealer is the deletion of Z from the access structure Γ_x. Similarly, if $Z \subseteq P$ is unqualified, then the access structure induced by the matroid M/Z with x as the dealer is the contraction of Z from the access structure Γ_x.

When a matroid-induced access structure is ideal, there is a nice correspondence between rank and entropy.

Theorem 2.52 ([15]). *Let Γ_x be an ideal access structure induced by the matroid M, and let Σ be an ideal scheme for Γ_x. Then the rank function of M is the normalized entropy function h obtained from Σ.*

Matroids are of interest in secret-sharing research because of their connections to ideal schemes. Brickell and Davenport proved that any access structure with an ideal scheme must be induced by a matroid, and also that suitably nice matroids, including representable ones, induce ideal schemes [6]. The result that any ideal access structure must be induced by a matroid was generalized by Martí-Farré and Padró, who proved that any access structure with information rate greater than $2/3$ must be induced by a matroid [19]. While non-representable matroids can induce access structures that are not ideal [1], there is as of yet no non-ideal access structure induced by a non-representable matroid for which the exact information rate is known.

2.10 Linear Secret Sharing

Recall that we are concerned only with random variables defined on finite probability spaces. In this section we use vector spaces as probability spaces. All vector spaces are assumed to be finite-dimensional over a finite field, and therefore finite.

Definition 2.53. Let X be a random variable defined on a probability space consisting of a finite vector space equipped with the uniform probability distribution. If X is a linear map onto a vector space, we say that X is a *linear random variable*.

Let W be a finite-dimensional vector space over a finite field K of size k. Then W is finite. Equip W with the uniform probability distribution, and let $X : W \to W_X$. Without loss of generality we assume X is surjective. We may think of X as projection from W to W_X.

Let $V = W^*$ and $V_X = W_X^*$. We may assume $V_X \subseteq V$ since W_X^* may be canonically embedded in W^*, via the map sending f to $f \circ X$. Since we are dealing with finite-dimensional vector spaces, we identify each vector space with its double dual and thus have $X : V^* \to V_X^*$, now thinking of X as projection from V^* to V_X^*. Because of the way V_X has been identified with a subspace of V, we may identify the projection X with restriction: given $f \in V^*$, $X(f)$ is the restriction of f to V_X.

When given a collection of linear random variables on the same probability space, for each random variable X there is an associated subspace V_X. Conversely, for any subspace V_X of V we define the linear random variable $X : V^* \to V_X^*$ by letting X send $f \in V^*$ to the restriction of f to V_X. This association between subspaces and linear random variables allows us to talk about the intersection of individual linear random variables, which is something we cannot do for general non-linear random variables. The intersection of two linear subspaces is again a linear subspace. This means for any two linear random variables X and Y there is a well-defined random variable $X \cap Y$ with corresponding subspace $V_X \cap V_Y$.

For any two linear random variables X and Y there is also a random variable XY whose corresponding linear subspace is the vector sum of subspaces $V_X + V_Y$. By induction, any finite set X of linear random variables may be identified with the single random variable V_X whose corresponding linear subspace is the linear span of the subspaces for for the individual random variables.

For sets X, Y of linear random variables, there are two different notions of intersection. Using set intersection as we do for non-linear random variables, we could let Z be the set intersection of X and Y with associated subspace V_Z. However, we will not use this definition. Instead, we associate to X and Y the subspaces V_X and V_Y in the manner explained above, and let $Z = X \cap Y$ have as its associated subspace

the intersection of subspaces $V_X \cap V_Y$.

With the given notions of union and intersection, the entropy function behaves nicely for linear random variables. Let $X : W \to W_X$ be a linear random variable and let V be such that $W = V^*$ and $W_X = V_X^*$, as above. Use $\dim(\cdot)$ to denote the dimension of a subspace. Since W is equipped with the uniform distribution and each element of W_X will have an equal number of preimages under X, any element of W_X is equally likely to be the value of the random variable X. Since we are dealing with finite vector spaces,

$$\dim(W_X) = \dim(V_X^*) = \dim(V_X)$$

and so the size of W_X is $k^{\dim(V_X)}$. Thus by Lemma 2.12,

$$H(X) = \log k^{\dim(V_X)} = \dim(V_X)\log(k).$$

Since $\log(k)$ is constant over all linear subspaces of V, $H(X)$ corresponds to the dimension of the subspace V_X.

Remark 2.54. Recall that for linear subspaces V_X, V_Y

$$\dim(V_X) + \dim(V_Y) = \dim(V_X \cap V_Y) + \dim(V_X + V_Y).$$

From the correspondence between entropy and dimension of subspaces, it follows that the entropy function H is modular for any two individual linear random variables X, Y over $X \cap Y$, where $X \cap Y$ is as defined above:

$$H(X) + H(Y) = H(X \cap Y) + H(XY).$$

We now apply this notion of linearity to secret sharing schemes.

Definition 2.55. A *linear secret sharing scheme* is one in which the random variables for the secret and for all participants' shares are linear random variables.

Since linearity imposes additional restrictions on the entropy function, such as the modularity mentioned above, it is sometimes possible to prove stronger statements for linear schemes than for arbitrary secret sharing schemes.

CHAPTER 3

Information Inequalities

3.1 Types of Information Inequalities

One technique for bounding the information rate of a non-ideal access structure is to fix an arbitrary secret sharing scheme for that access structure and sum a suitable collection of inequalities satisfied by the corresponding entropy function. The goal is to arrive at an inequality that implies the information rate of some participant in the access structure must be bounded below 1. This chapter introduces different types of information inequalities, presents a way to visualize information inequalities, and shows some applications of information inequalities.

Definition 3.1. An *information inequality* is any inequality of the form

$$0 \leq \sum_{X \subseteq Y} C_X H(X)$$

that holds for the entropy functions of all collections Y of random variables.

Recall that information inequalities obtainable as a non-negative linear combination of monotonicity and submodularity inequalities are collectively called Shannon inequalities, or basic inequalities.

The Shannon inequalities do not account for all inequalities that must be satisfied by entropy functions.

Definition 3.2. A *non-Shannon inequality* is any inequality that must hold for all entropy functions, but cannot be obtained as a non-negative linear combination of basic inequalities.

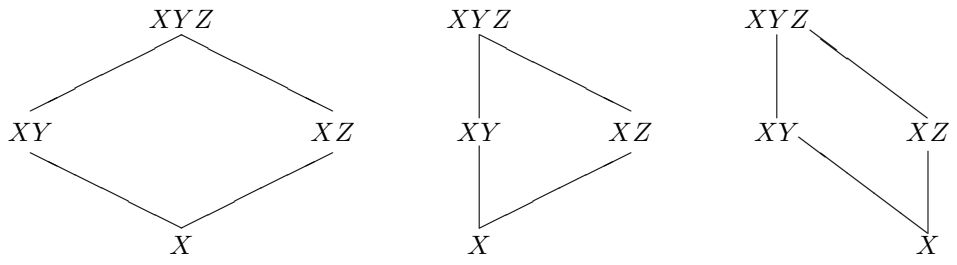
For some access structures, non-Shannon inequalities may be used to find better bounds for information rates than could be found using only Shannon inequalities.

In some cases we also use inequalities which do not always hold, but which are known to hold under certain additional assumptions on the random variables. The additional assumptions we impose on the random variables may include linearity and particular instances of modularity.

Any information inequality may of course be rewritten so that the left-hand, or smaller side, is 0. We will use interchangeably phrases such as "occurring negatively" and "occuring on the smaller side of the inequality." Similarly, we use interchangeably phrases such as "occurring positively" and "occuring on the larger side of the inequality."

When working in a secret sharing context, we may divide through any information inequality by $H(S)$ to get a corresponding normalized inequality that must be satisfied by the normalized entropy function h. We expand our definition of information inequalities to include, when appropriate, the corresponding inequalities for h. In particular, "Shannon inequalities" will include $+$-monotonicity and $+$-submodularity, since these result from monotonicity, submodularity, and the definition of a secret sharing scheme. Similarly, "non-Shannon inequalities" will include the normalized versions of non-Shannon inequalities. The general form of an information inequality for the normalized entropy function h is

$$a \leq \sum_{X \subseteq Y} C_X h(X)$$



(a) (b) (c)

Figure 3.1: Visual Representations of Submodularity

where a is a constant. In all information inequalities we consider here, a is non-negative.

3.2 Visual Representation of Information Inequalities

When adding a collection of Shannon inequalities it is often useful to draw visual representations of the inequalities we are adding, using the boolean lattice of subsets.

A diamond in the boolean lattice of subsets may be used to represent a submodularity inequality. For example, Figure 3.1(a) represents the inequality

$$H(X) + H(XYZ) \leq H(XY) + H(XZ).$$

Sets on the sides of the diamond are those whose entropies are counted positively in the inequality, while sets on the top and bottom of the diamond are those whose entropies are counted negatively. At times we will find it convenient to draw rather misshapen diamonds, as in Figure 3.1(b) and (c).

To add submodularity inequalities, we draw a representation with a diamond for each inequality. For each set X in the representation we count the number of diamonds for which X occurs on a side, then subtract the number of diamonds for which X occurs on the top or the bottom. This gives the coefficient of $H(X)$ in the sum of the inequalities.

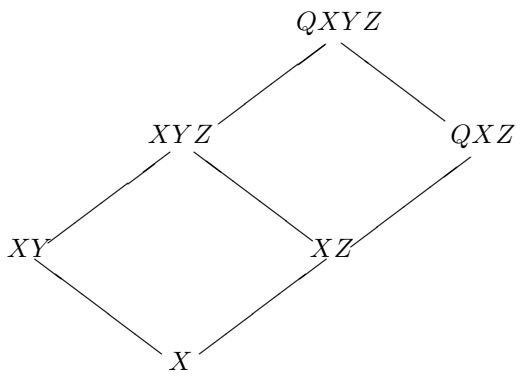


Figure 3.2: Visual Representation of the Sum of Two Submodularity Inequalities for H

Example 3.3. Figure 3.2 represents the sum of the submodularity inequalities

$$H(X) + H(XYZ) \leq H(XY) + H(XZ)$$

and

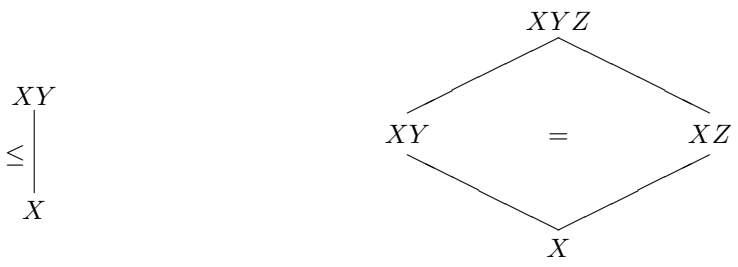
$$H(XZ) + H(QXYZ) \leq H(XYZ) + H(QXZ).$$

We see that the set XZ occurs on the side of one diamond and on the bottom of another. Thus in the sum of the corresponding inequalities, $H(XZ)$ will have coefficient 0. Similarly, $H(XYZ)$ will have coefficient 0. The sets XY and QXZ each occur on the side of one diamond, so their entropies will each have coefficient 1. The sets X and $QXYZ$ each occur on the bottom or top, respectively, of one diamond, so their entropies will each have coefficient -1. Thus the final sum of inequalities is

$$0 \leq H(XY) + H(QXZ) - H(X) - H(QXYZ).$$

If we add the inequalities directly without using the picture, we get the equivalent inequality

$$H(X) + H(QXYZ) \leq H(XY) + H(QXZ).$$



(a) Monotonicity: $H(X) \leq H(XY)$ (b) Modularity: $H(XY) + H(XZ) = H(X) + H(XYZ)$

Figure 3.3: Extensions to Our System of Visual Representations

While this example is small enough that one can easily add the inequalities without a picture, in later sections we will perform larger computations for which visual representations will save work.

Remark 3.4 (Visual Representation of Mutual Information). We can also use diamonds in the boolean lattice of subsets to represent mutual information and conditional mutual information. For example, Figure 3.1 may also be thought of as giving visual representations for

$$I(Y;Z|X) = H(XY) + H(XZ) - H(X) - H(XYZ).$$

Such representations can be helpful for checking the validity of equations involving mutual information and conditional mutual information. Figure 3.2 illustrates the validity of the equation

$$I(Y;Z|X) + I(Y;Q|XZ) = I(Y;QZ|X).$$

Our visual representations are not limited to submodularity. When we wish to include monotonicity, we simply include a $\leq$ sign as in Figure 3.3(a). In situations where we need to indicate modularity, we include an $=$ sign in the appropriate diamond, as in Figure 3.3(b).

For complex pictures and those with modularity, it may be helpful to label each set with a "+" for each time it is on a side of a diamond, and a "−" for each time it

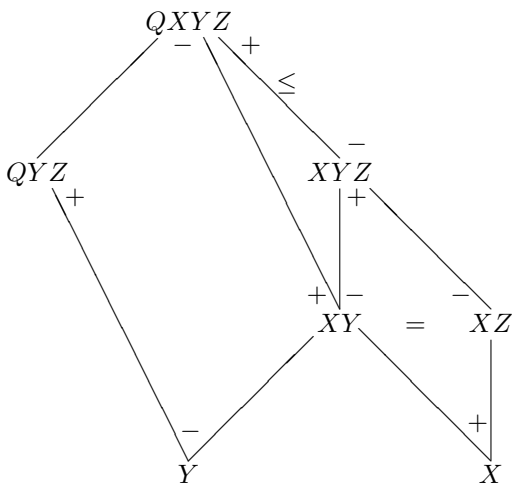


Figure 3.4: Visual Representation of a Sum of Inequalities for H

is on a top or bottom. This will make it easier to determine each coefficient in the final sum of inequalities.

Example 3.5. Figure 3.4 represents the sum of the inequalities and modularity equation

$$\begin{aligned} H(Y) + H(QXYZ) &\leq H(QYZ) + H(XY) \\ H(XYZ) &\leq H(QXYZ) \\ H(XY) + H(XZ) &= H(X) + H(XYZ). \end{aligned}$$

We leave it as an exercise to check that whether one counts + and − signs in the picture, or adds the inequalities without the picture, the sum is

$$H(Y) + H(XZ) \leq H(X) + H(QYZ).$$

The visual notation we have introduced to represent inequalities for H may also be used to represent the corresponding inequalities for normalized entropy, where each H is replaced with h. For working in a secret sharing context with normalized entropy we introduce two additional pieces of notation. To indicate a qualified set

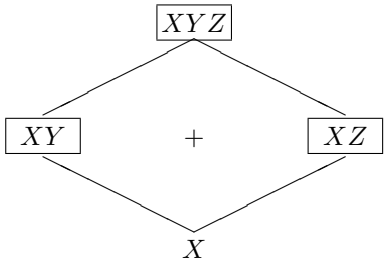


Figure 3.5: Visual Representation of +-Submodularity

we draw a box around its name, and to indicate +-submodularity we further draw a "plus" sign in the appropriate diamond. Thus Figure 3.5. represents the inequality

$$h(X) + h(XYZ) + 1 \quad \leq \quad h(XY) + h(XZ).$$

where $X \notin \Gamma$ but $XY, XZ \in \Gamma$.

To use these visual representations to find a sum of inequalities for h, we determine the coefficient for each term $h(X)$ as before. In addition, we may now have a non-zero constant on the smaller side of the inequality. If this is the case, the constant term will be the number of diamonds in the picture containing a "+" sign.

Example 3.6. Figure 3.6 represents the sum of the inequalities

$$h(X) + h(XYZ) \leq h(XY) + h(XZ)$$

and

$$h(XZ) + h(QXYZ) + 1 \leq h(XYZ) + h(QXZ).$$

These inequalities arise respectively from submodularity and from +-submodularity in a situation where $XZ \notin \Gamma$ but $XYZ, QXZ \in \Gamma$. As in Example 3.3, the terms $h(XZ)$ and $h(XYZ)$ will each have coefficient 0, while the normalized entropies of the other sets will have coefficients of 1 or -1 as appropriate. Since there is one diamond resulting from +-submodulariy, we will have a constant term of 1 on the

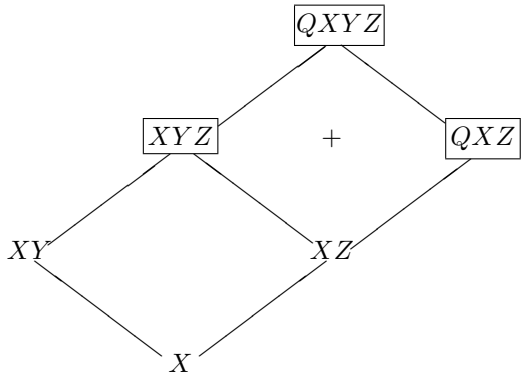


Figure 3.6: Visual Representation of a Sum of Inequalities for h

smaller side of the sum of inequalities. Putting everything together, the final sum of inequalities is

$$1 \leq h(XY) + h(QXZ) - h(X) - h(QXYZ).$$

3.3 A Generating Set of Shannon Inequalities

For a given collection of random variables there are many Shannon inequalities. For some situations it is helpful to have a smaller generating set of Shannon inequalities.

Any submodularity inequality may be obtained as a sum of submodularity inequalities of the form

$$H(X) + H(X \cup \{a, b\}) \leq H(X \cup \{a\}) + H(X \cup \{b\}). \tag{3.1}$$

To see this, consider an arbitrary submodularity inequality

$$H(Z) + H(XYZ) \leq H(XZ) + H(YZ). \tag{3.2}$$

Write

$$X = Z \cup \{x_1, \ldots, x_m\} \text{ and } Y = Z \cup \{y_1, \ldots, y_m\},$$

and let

$$X_i = \{x_1, \ldots, x_i\} \text{ and } Y_j = \{y_1, \ldots, y_j\}.$$

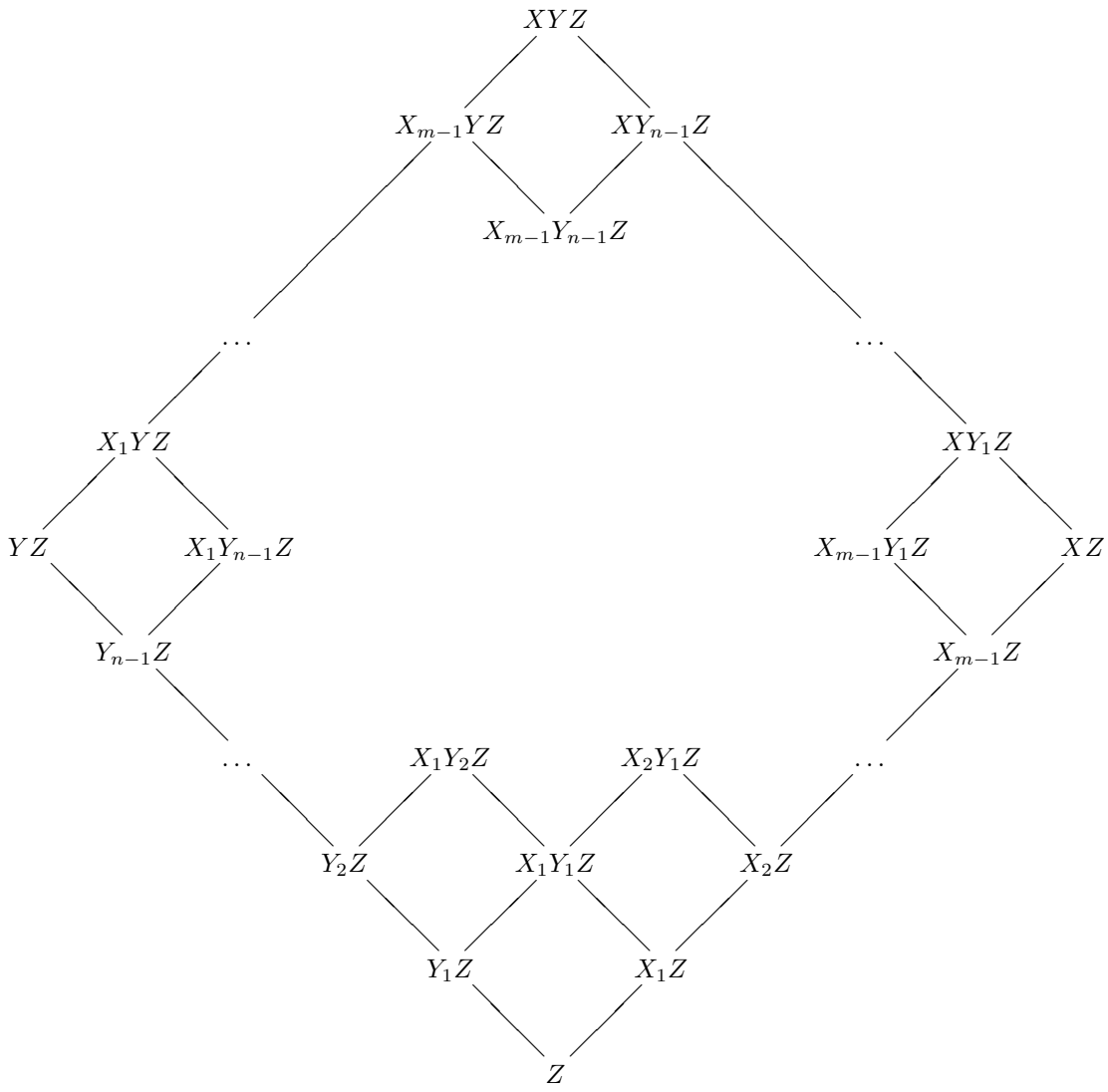


Figure 3.7: Generation of a Submodularity Inequality

Then Figure 3.7 shows inequalities of the form given in inequality (3.1) whose sum is inequality (3.2).

Once all submodularity inequalities have been generated, we need only a small set of monotonicity inequalities to generate the remaining monotonicity inequalities. Consider a set $Y = \{y_1, \ldots, y_n\}$ of random variables. All monotonicity inequalities that hold between subsets of Y can be obtained by combining inequalities of the

form

$$H(X) \leq H(X \cup \{y_i\}), \tag{3.3}$$

where X is an arbitrary subset of Y and $y_i \in Y \setminus X$. Since inequality (3.3) is the sum of the submodularity inequality

$$H(X) + H(XY) \leq H(X \cup \{y_i\}) + H(XY \setminus \{y_i\})$$

and the monotonicity inequality

$$H(Y \setminus \{y_i\}) \leq H(Y), \tag{3.4}$$

submodularity and monotonicity inequalities of the form shown in (3.4) will generate the remaining monotonicity inequalities. To summarize, the collection of all submodularity inequalities of the form (3.1) and all monotonicity inequalities of the form (3.4) is a generating set for the collection of all Shannon inequalities.

When we work in a secret sharing context with the function h, we get a generating set of Shannon inequalities by dividing through all inequalities of the forms (3.1) and (3.4) by $H(S)$ to get inequalities for h, and combining these with all +-submodularity inequalities of the form

$$h(X) + h(X \cup \{a, b\}) + 1 \leq h(X \cup \{a\}) + h(X \cup \{b\}) \tag{3.5}$$

where $X \cup \{a\}$ and $X \cup \{b\}$ are qualified but X is not.

An arbitrary +-submodularity such as

$$h(Z) + h(XYZ) + 1 \leq h(XZ) + h(YZ)$$

will be a sum of inequalities as represented in Figure 3.7, with the addition that now one of the mn small diamonds will contain a "+". To find such a diamond, take a

maximal unqualified set of XYZ including Z. Without loss of generality we may assume this maximal unqualified set is of the form X_iY_jZ for some i, j. Then a "plus 1" will be contributed by the inequality corresponding to the diamond with X_iY_jZ on the bottom and $X_{i+1}Y_jZ$, $X_iY_{j+1}Z$ on the sides. This inequality will be of the form (3.5).

It turns out that +-monotonicity is a special case of +-submodularity. Let X be unqualified and XY be qualified. Then the +-monotonicity

$$h(X) + 1 \leq h(XY)$$

is obtained by simplifying the +-submodularity

$$h(X) + h(XY) + 1 \leq h(XY) + h(XY).$$

We conclude that all Shannon inequalities for the normalized entropy function are generated by those submodularity and monotonicity inequalities obtained by dividing through (3.1) and (3.2) by $H(S)$, combined with those +-submodularities of the form shown in (3.5).

3.4 Independent Sequences

For another example where visual representations can be quite useful, we consider the independent sequences introduced in [5].

Definition 3.7 ([5])**.** Given an access structure Γ on participants P, a sequence of participants $B = b_1, \ldots, b_m$ is called an *independent sequence* if

1. $\{b_1, \ldots, b_m\} \notin \Gamma$
2. there exist m non-empty subsets $X_i \subseteq P$ such that:
   (a) $\{b_1, \ldots, b_i\} \cup X_i \in \Gamma$ for $i = 1, \ldots, m$, and

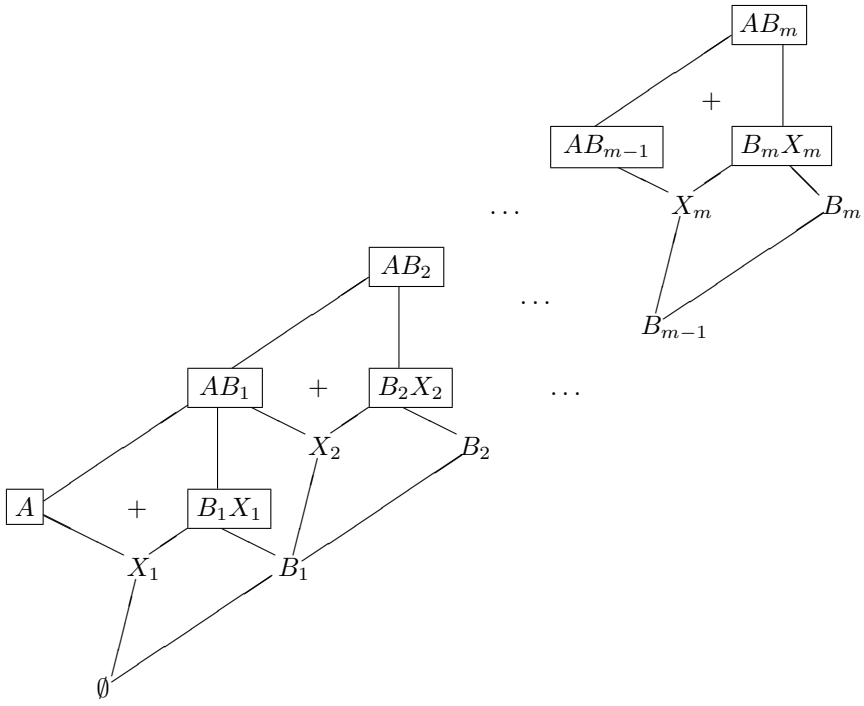


Figure 3.8: Visual Representation of Independent Sequence where $A \in \Gamma$

(b) $\{b_1, \ldots, b_{i-1}\} \cup X_i \notin \Gamma$ for $i = 1, \ldots, m$.

Let $A \subseteq P$ be a subset of participants such that $X_i \subseteq A$ for any $i = 1, \ldots, m$. Then the set A *makes the sequence* B *independent.*

The main result involving independent sequences is the following theorem, which we write in terms of normalized entropy. Our proof of this theorem illustrates how useful visual representations can be for summing large collections of information inequalities.

Theorem 3.8 ([5])**.** *Let* $B = b_1, \ldots, b_m$ *be an independent sequence of* Γ *and let* $A \subseteq P$ *be a set of participants that makes* B *independent. Then*

$$h(A) \geq \begin{cases} (m+1) & \text{if } A \in \Gamma \\ m & \text{if } A \notin \Gamma. \end{cases}$$

Proof. Let $B_i = \{b_1, \ldots, b_i\}$.

First, assume A is qualified. This assumption and the definition of independent sequence imply the +-submodularity inequalities shown in Figure 3.8. Below each +-submodularity diamond we have another diamond, with a qualified set at the top and unqualified sets on both sides, resulting from the submodularity of the normalized entropy. If we add the inequalities represented by these diamonds, we can see from the picture that the entropies of all sets except those on the outermost corners will cancel out. We thus obtain

$$h(AB_m) + m \leq h(A) + h(B_m). \tag{3.6}$$

The set B_m is by assumption not qualified, whereas AB_m contains $X_m B_m$ and is therefore qualified. By +-monotonicity,

$$h(B_m) + 1 \leq h(AB_m).$$

Adding this to Equation (3.6) and canceling terms, we obtain

$$m + 1 \leq h(A) \text{ when } A \in \Gamma.$$

If A is unqualified, we will have submodularity instead of +-submodularity in the diamond with sides A and B_1X_1, so instead of Equation (3.6) we will have

$$h(AB_m) + (m-1) \leq h(A) + h(B_m).$$

Again, we add

$$h(B_m) + 1 \leq h(AB_m)$$

and cancel terms. In this case we obtain

$$m \leq h(A) \text{ when } A \notin \Gamma.$$

□

3.5 Ingleton's Inequality

Ingleton's Inequality is known to be satisfied by the entropy function on any set of four linear random variables. This inequality has been used to prove bounds on the information rates of linear secret sharing schemes for certain access structures. We present a pictorial proof of Ingleton's Inequality for linear random variables, and then show that the linearity assumption can be replaced by a suitable independence assumption.

Definition 3.9. *Ingleton's Inequality for A,D over B,C* is the inequality

$$H(B) + H(C) + H(AD) + H(ABC) + H(BCD) \leq H(AB) + H(AC) + H(BC) + H(BD) + H(CD).$$

Theorem 3.10. *If A, B, C, D are linear random variables, then Ingleton's Inequality holds for A, D over B, C.*

Proof. Our proof is a slight alteration of that given by Ingleton in [13]. Consider Figures 3.9 and 3.10. The diamonds marked with "=" result from the modularity of entropy on linear random variables, as discussed in Remark 2.54. The sum of the inequalities represented by Figures 3.9 and 3.10 is Ingleton's Inequality. □

One may reasonably ask under what circumstances Ingleton's Inequality holds for non-linear random variables. The proof given above does not immediately translate to the non-linear case, as we do not have a definition for the "intersection" of non-linear random variables. However, on closer inspection, the proof of Ingleton's Inequality for linear random variables relies only on the modularity conditions that hold for dimensions of intersections and unions of linear subspaces. It follows that Ingelton's Inequality will hold for non-linear random variables if we make sufficiently

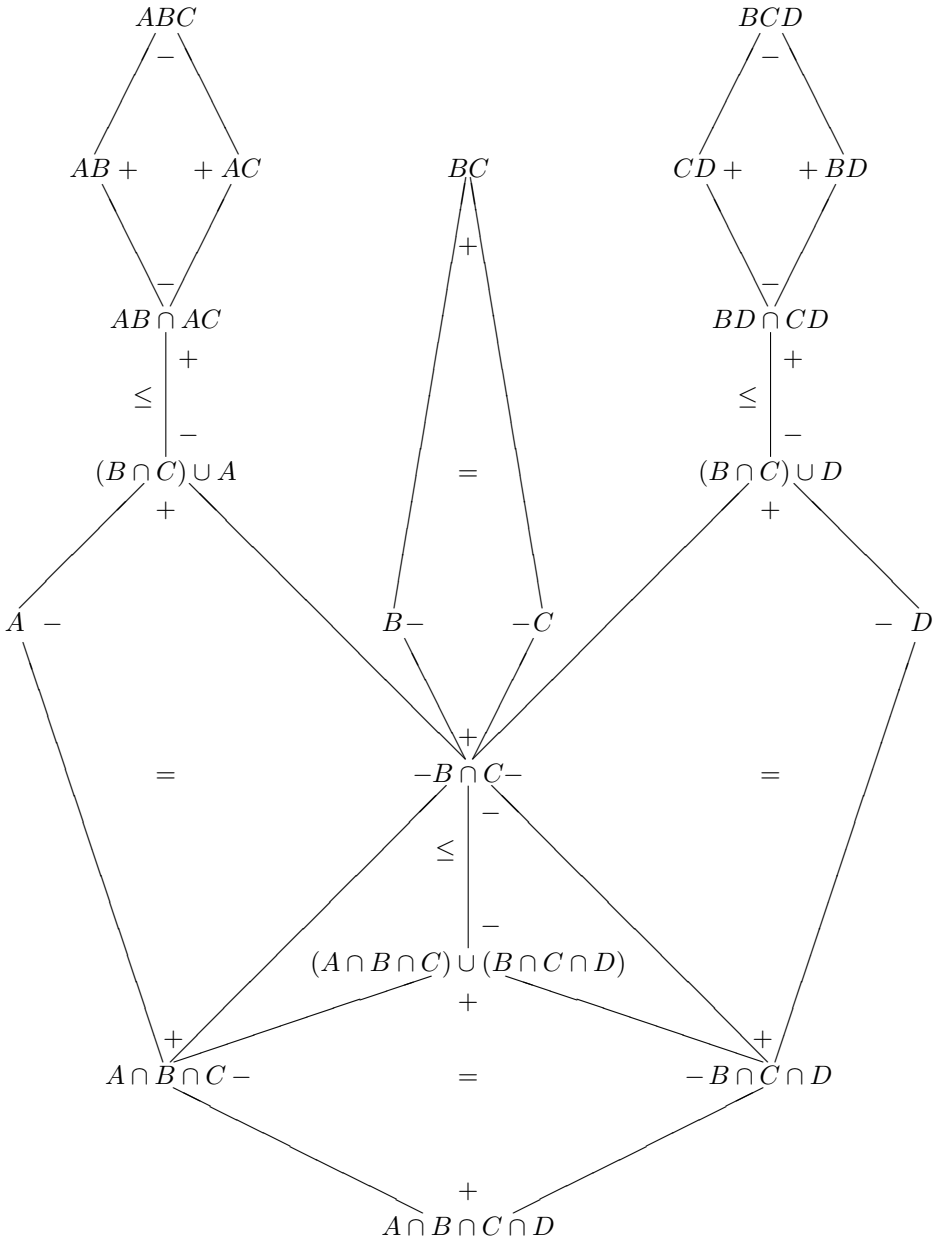


Figure 3.9: Visual Representation of the Proof of Ingleton's Inequality

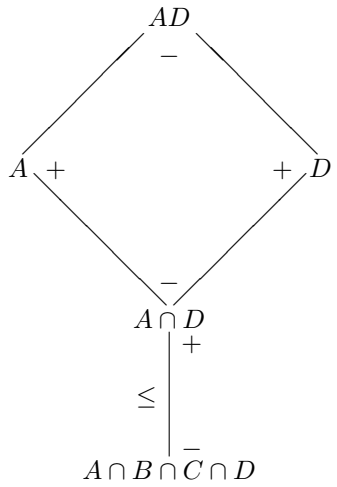


Figure 3.10: Visual Representation of the Proof of Ingleton's Inequality, cont.

strong independence assumptions. Recall that we say A and D are independent given B and C if A, B, C, D are random variables such that $I(A; D|BC) = 0$.

Theorem 3.11. *If (1) A and D are independent given B and C, or if (2) B and C are independent, then Ingleton's Inequality holds for A, D over B, C.*

Proof. Case 1: Suppose $I(A; D|BC) = 0$. Then

$$0 = I(A; D|BC) = H(ABC) + H(BCD) - H(BC) - H(ABCD),$$

and so

$$H(ABC) + H(BCD) = H(BC) + H(ABCD).$$

Add to this equation the following three inequalities, results of submodularity:

$$H(AD) + H(ABCD) \leq H(ABD) + H(ACD)$$

$$H(ABD) + H(B) \leq H(AB) + H(BD)$$

$$H(ACD) + H(C) \leq H(AC) + H(CD).$$

A visual representation is shown in Figure 3.11. After cancelling terms we obtain Ingleton's Inequality.

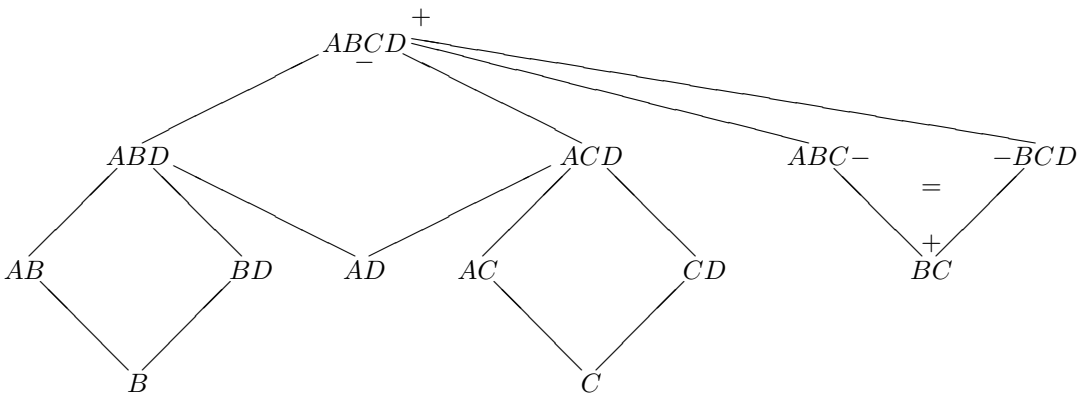


Figure 3.11: Proof of Ingleton's Inequality Assuming $I(A; D|BC) = 0$

Case 2: Suppose $I(B; C) = 0$. Then add to the resulting equation

$$H(B) + H(C) = H(BC)$$

the three submodularity inequalities

$$H(AD) \leq H(A) + H(D)$$

$$H(A) + H(ABC) \leq H(AB) + H(AC)$$

$$H(D) + H(BCD) \leq H(BD) + H(CD).$$

A visual representation of the equation and inequalities is given in Figure 3.12. After cancelling terms we obtain Ingleton's Inequality. □

Matúš also proves that Ingleton's Inequality holds under certain independence conditions [17].

Theorem 3.12. *Assume $I(A; D|B) = 0$. If either $I(A; D) = 0$ or $I(C; D|B) = 0$, then Ingleton's Inequality holds for A, D over B, C.*

The conditions Matúš requires need not hold under the hypotheses of Theorem 3.11, as illustrated by the following two examples.

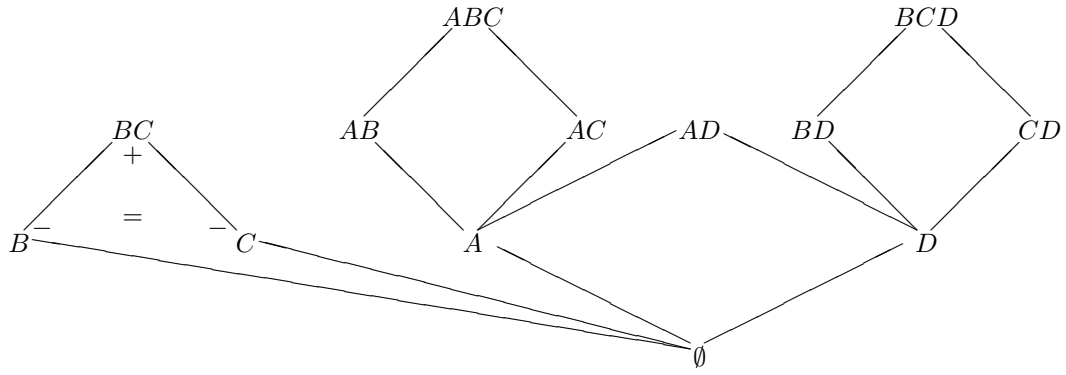


Figure 3.12: Proof of Ingleton's Inequality Assuming $I(B;C) = 0$

Example 3.13. First we show how to select random variables A, B, C, D so that

$$I(A; D|BC) = 0 \text{ but } I(A; D|B) > 0.$$

Let A and B be independent random variables with positive entropies taking values in $\mathbb{Z}_n$ for some $n > 1$. Let $C = A - B$ and let $D = C$. Then since B and C together determine A,

$$\begin{aligned} H(BC) =& H(ABC) \\ H(BCD) =& H(ABCD). \end{aligned}$$

It follows that

$$I(A; D|BC) = H(ABC) - H(BC) + H(BCD) - H(ABCD) = 0.$$

However, since $D = C$ and since B and C together determine A, $H(BC) = H(ABC)$ and so

$$\begin{aligned} I(A; D|B) =& H(AB) + H(BD) - H(B) - H(ABD) \\ =& H(AB) + H(BC) - H(B) - H(ABC) \\ =& H(AB) - H(B). \end{aligned}$$

Since A and B were chosen independently, $H(AB) = H(A) + H(B)$. Since by assumption $H(A)$ is positive, we conclude that

$$I(A; D|B) = H(A) > 0.$$

Example 3.14. Now we show how to select random variables A, B, C, D so that

$$I(B; C) = 0 \text{ but } I(A; D|B) > 0.$$

Let A, B, and C be chosen independently, each with positive entropy, and let $D = A$. $I(B; C) = 0$ is immediate. Since $A = D$, also $H(ABD) = H(BD)$ and thus

$$\begin{aligned} I(A; D|B) =& H(AB) + H(BD) - H(B) - H(ABD) \\ =& H(AB) - H(B). \end{aligned}$$

As in the previous example, since A and B were chosen independently and with positive entropies, this quantity is strictly greater than zero.

3.6 A New Proof of the Zhang-Yeung Inequality

The first known non-Shannon inequality was the Zhang-Yeung inequality [33]. We present a new proof of the Zhang-Yeung inequality, making use of Ingleton's Inequality.

Theorem 3.15 (Zhang-Yeung Inequality)**.** *For random variables A, B, C, D*

$$\begin{aligned} &H(A) + 2H(B) + 2H(C) + H(AD) + 4H(ABC) + H(BCD) \\ &\qquad \leq 3H(AB) + 3H(AC) + 3H(BC) + H(CD) + H(BD). \end{aligned}$$

Proof. Let X, Y be random variables such that the joint distribution of $ABCD$ and the joint distribution of $XBCY$ are identical, and such that $I(AD; XY|BC) = 0$. We think of X, Y as being copies of A and D, while B and C are held fixed.

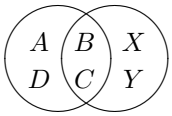


Figure 3.13: X, Y as Copies of A, D over B, C

By the definition of mutual information one can confirm that

$$I(AD; XY|BC) = I(A; X|BC) + I(D; X|ABC) + I(A; Y|XBC) + I(D; Y|ABCX).$$

Since mutual information of two random variables is non-negative, each term on the right-hand side of the above equation must equal zero. Then $I(A; X|BC) = 0$, and so Ingleton's Inequality holds for A, X over B, C:

$$H(B) + H(C) + H(AX) + H(ABC) + H(BCX) \leq H(AB) + H(AC) + H(BC) + H(BX) + H(CX). \tag{3.7}$$

Similarly, $I(A; Y|BC) = 0$ and so Ingleton's Inequality also holds for A, Y over B, C:

$$H(B) + H(C) + H(AY) + H(ABC) + H(BCY) \leq H(AB) + H(AC) + H(BC) + H(BY) + H(CY). \tag{3.8}$$

A different rewriting of the mutual information gives

$$I(AD; XY|BC) = I(A; XY|BC) + I(D; XY|ABC)$$

and so $I(A; XY|BC) = 0$. Thus

$$H(ABC) + H(BCXY) = H(BC) + H(ABCXY). \tag{3.9}$$

We now add inequalities (3.7), (3.8), (3.9), and the following two Shannon in-

equalities:

$$H(ABCXY) + H(XY) \leq H(AXY) + H(BCXY)$$
$$H(A) + H(AXY) \leq H(AX) + H(AY).$$

Cancelling terms leaves

$$H(A) + 2H(B) + 2H(C) + 3H(ABC) + H(BCX) + H(BCY) + H(XY)$$
$$\leq 2H(AB) + 2H(AC) + 3H(BC) + H(BX) + H(BY) + H(CX) + H(CY).$$

By our assumption that the joint distributions on $ABCD$ and $XBCY$ are identical, we can make the following substitutions:

$$H(XY) = H(AD)$$
$$H(XB) = H(AB)$$
$$H(XC) = H(AC)$$
$$H(XBC) = H(ABC)$$
$$H(YB) = H(BD)$$
$$H(YC) = H(CD)$$
$$H(YBC) = H(BCD).$$

After collecting terms and rearranging, we are left with the Zhang-Yeung inequality.

□

3.7 More Non-Shannon Inequalities

Consider a set P of random variables and an information inequality

$$0 \leq \sum_{X \subseteq P} C_X h(X).$$

Inequality	Permutation(s) Performed
ZY98	$B \leftrightarrow D$
DFZ(i)	none
DFZ(ii)	$B \leftrightarrow D$
DFZ(iii)	$A \leftrightarrow B$, then $B \leftrightarrow C$
DFZ(iv)	none
DFZ(v)	none
DFZ(vi)	$A \leftrightarrow C$

Table 3.1: Permutations of Letters in DFZ Inequalities

Definition 3.16. For a set $X \subseteq P$ we define the *upward sum* $\uparrow(X)$ and the *downward sum* $\downarrow(X)$ for the given information inequality as follows:

$$\uparrow(X) = \sum_{Y \supseteq X} C_Y$$

$$\downarrow(X) = \sum_{Y \subseteq X} C_Y.$$

The numbers we obtain as upward and downward sums are in general nicer (of smaller magnitude) than the original coefficients. In Chapter 4, Section 4.5 we will use the upward and downward sums to help prove bounds on information rates.

Tables 3.2 and 3.3 show the coefficients, upward sums, and downward sums for the Zhang-Yeung inequality [33] and the six additional non-Shannon inequalities in [9]. So that the inequalities as shown here would take a consistent form, we permuted some letters in the inequalities as shown in [9]. The permutations performed are shown in Table 3.1.

Table 3.4 shows the coefficients and upward and downward sums for the two infinite sequences of information inequalities from Corollary 3 in [18]. For the sake of consistent notation, we use letters in place of Matúš' numbers. In the first inequality the letters A, B, C, D correspond respectively to the numbers 1,3,4,2 in [18]. In the second inequality the letters A, B, C, D correspond respectively to 2,3,4,1. Here s is a positive integer enumerating the inequalities.

	ZY98			**DFZ(i)**			**DFZ(ii)**			**DFZ(iii)**		
X	C_X	$\downarrow(X)$	$\uparrow(X)$	C_X	$\downarrow(X)$	$\uparrow(X)$	C_X	$\downarrow(X)$	$\uparrow(X)$	C_X	$\downarrow(X)$	$\uparrow(X)$
A	-1	-1	0	-3	-3	0	-2	-2	0	-2	-2	0
B	-2	-2	0	-5	-5	0	-3	-3	0	-7	-7	0
C	-2	-2	0	-3	-3	0	-5	-5	0	-4	-4	0
D	0	0	0	0	0	0	-1	-1	0	0	0	0
AB	3	0	-1	8	0	-1	5	0	-2	8	-1	-1
AC	3	0	-1	6	0	-3	6	-1	-1	5	-1	-4
AD	-1	-2	-1	-2	-5	-2	-2	-5	-2	-2	-4	-2
BC	3	-1	-2	6	-2	-5	6	-2	-5	9	-2	-4
BD	1	-1	0	2	-3	0	3	-1	-1	3	-4	-1
CD	1	-1	0	2	-1	0	4	-2	0	3	-1	-1
ABC	-4	0	-4	-9	0	-9	-7	0	-7	-9	0	-9
ABD	0	0	0	0	0	0	0	0	0	0	0	0
ACD	0	0	0	0	0	0	0	0	0	0	0	0
BCD	-1	0	-1	-2	0	-2	-4	0	-4	-4	0	-4
$ABCD$	0	0	0	0	0	0	0	0	0	0	0	0

Table 3.2: Coefficients, Downward Sums, and Upward Sums for ZY98, DFZ(i), DFZ(ii), DFZ(iii)

	DFZ(iv)			**DFZ(v)**			**DFZ(vi)**		
X	C_X	$\downarrow(X)$	$\uparrow(X)$	C_X	$\downarrow(X)$	$\uparrow(X)$	C_X	$\downarrow(X)$	$\uparrow(X)$
A	-1	-1	0	-1	-1	0	-1	-1	0
B	-5	-5	0	-7	-7	0	-5	-5	0
C	-5	-5	0	-4	-4	0	-5	-5	0
D	0	0	0	-1	-1	0	0	0	0
AB	6	0	-3	7	-1	-2	5	-1	-2
AC	6	0	-3	5	0	-4	5	-1	-2
AD	-2	-3	-2	-2	-4	-2	-2	-3	-2
BC	8	-2	-3	9	-2	-4	8	-2	-3
BD	2	-3	0	4	-4	0	3	-2	-1
CD	2	-3	0	3	-2	-1	3	-2	-1
ABC	-9	0	-9	-9	0	-9	-7	0	-7
ABD	0	0	0	0	0	0	0	0	0
ACD	0	0	0	0	0	0	0	0	0
BCD	-2	0	-2	-4	0	-4	-4	0	-4
$ABCD$	0	0	0	0	0	0	0	0	0

Table 3.3: Coefficients, Downward Sums, and Upward Sums for DFZ(iv), DFZ(v), and DFZ(vi)

	First Inequality			Second Inequality		
X	C_X	$\downarrow(X)$	$\uparrow(X)$	C_X	$\downarrow(X)$	$\uparrow(X)$
A	0	0	0	$\frac{-s(s-1)}{2}$	$\frac{-s(s-1)}{2}$	0
B	$\frac{-s(s+3)}{2}$	$\frac{-s(s+3)}{2}$	0	$\frac{-s(s+3)}{2}$	$\frac{-s(s+3)}{2}$	0
C	$-(s+1)$	$-(s+1)$	0	$-(s+1)$	$-(s+1)$	0
D	$\frac{-s(s+1)}{2}$	$\frac{-s(s+1)}{2}$	0	$-s$	$-s$	0
AB	s	$\frac{-s(s+1)}{2}$	0	s^2	$-s$	0
AC	s	-1	0	$\frac{s(s+1)}{2}$	-1	$\frac{-s(s-1)}{2}$
AD	$-s$	$\frac{-s(s+3)}{2}$	$-s$	$-s$	$\frac{-s(s+3)}{2}$	$-s$
BC	$\frac{(s+1)(s+2)}{2}$	$-s$	$\frac{-s(s+3)}{2}$	$\frac{(s+1)(s+2)}{2}$	$-s$	$\frac{-s(s+3)}{2}$
BD	$s(s+2)$	0	-1	$3s$	$\frac{-s(s-1)}{2}$	-1
CD	$\frac{(s+1)(s+2)}{2}$	0	$\frac{-s(s+1)}{2}$	$2s+1$	0	$-s$
ABC	$-s$	0	$-s$	$-s^2$	0	$-s^2$
ABD	0	0	0	0	0	0
ACD	0	0	0	0	0	0
BCD	$-(s+1)^2$	0	$-(s+1)^2$	$-(3s+1)$	0	$-(3s+1)$
$ABCD$	0	0	0	0	0	0

Table 3.4: Coefficients, Downward Sums, and Upward Sums for Matúš' Inequalities

Table 3.5 shows the coefficients for an inequality of the form found by Xu, Wang, and Sun in [31]. The letters A, B, C, D correspond to their numbers $3, 1, 2, 4$ respectively. We use their notation

$$\begin{aligned} S_+ &= \left(2+\sqrt{2}\right)^s \\ S_- &= \left(2-\sqrt{2}\right)^s. \end{aligned}$$

Again, s is a positive integer enumerating the inequalities.

X	C_X
A	-1
B	$2^{(s-1)} - \frac{\sqrt{2}}{4}S_+ + \frac{\sqrt{2}}{4}S_-$
C	$2^{(s-1)} - \frac{\sqrt{2}}{4}S_+ + \frac{\sqrt{2}}{4}S_-$
D	0
AB	$\frac{1}{4}S_+ + \frac{1}{4}S_-$
AC	$\frac{1}{4}S_+ + \frac{1}{4}S_-$
AD	$1 - 2^{(s-1)}$
BC	$1 - 3 \cdot 2^{(s-1)} + \frac{\sqrt{2}}{2}S_+ - \frac{\sqrt{2}}{2}S_-$
BD	$\frac{\sqrt{2}-1}{4}S_+ - \frac{\sqrt{2}+1}{4}S_-$
CD	$\frac{\sqrt{2}-1}{4}S_+ - \frac{\sqrt{2}+1}{4}S_-$
ABC	$2^{(s-1)} - \frac{1}{2}S_+ - \frac{1}{2}S_-$
ABD	0
ACD	0
BCD	$-(1 - 2^{(s-1)} + \frac{\sqrt{2}-1}{2}S_+ - \frac{\sqrt{2}+1}{2}S_-)$
$ABCD$	0

Table 3.5: Coefficients for the Inequalities Found by Xu, Wang, and Sun

CHAPTER 4

Upper Bounds for the Information Rates of Access Structures Induced By the Vámos Matroid, and Others

4.1 The Vámos Matroid and Induced Access Structures

The Vámos matroid on the set $\{v_1, \ldots, v_8\}$ is the matroid whose independent sets are all sets of size less than 5 except for the sets $\{v_1, v_2, v_3, v_4\}$, $\{v_1, v_2, v_5, v_6\}$, $\{v_3, v_4, v_5, v_6\}$, $\{v_3, v_4, v_7, v_8\}$, and $\{v_5, v_6, v_7, v_8\}$, which are circuits. We call the sets $\{v_1, v_2\}$, $\{v_3, v_4\}$, $\{v_5, v_6\}$, and $\{v_7, v_8\}$ *Vámos pairs*. Notice that each size 4 dependent set is a union of two Vámos pairs. Any set of fewer than 4 elements is independent, and any set with more than four elements is dependent. In the following discussion when we speak about circuits, independent sets, and dependent sets, we mean these terms with respect to the Vámos matroid. Since the Vámos matroid is not representable [20] it is not possible to draw a true visual representation of it, but Figure 4.1 may help with the intuition. Note that $\{v_1, v_2, v_7, v_8\}$ is not a plane.

Because of symmetries there are, up to isomorphism, only two access structures induced by the Vámos matroid. One is the structure V_1, where v_1 is the dealer. The other is V_6, where v_6 is the dealer. We consider each of V_1 and V_6 to be an access structure on eight participants, with the dealer being individually qualified to recover the secret (see Remark 2.29). The other minimal qualified sets will be those sets of non-dealer participants who, with the inclusion of the dealer, form a circuit in the

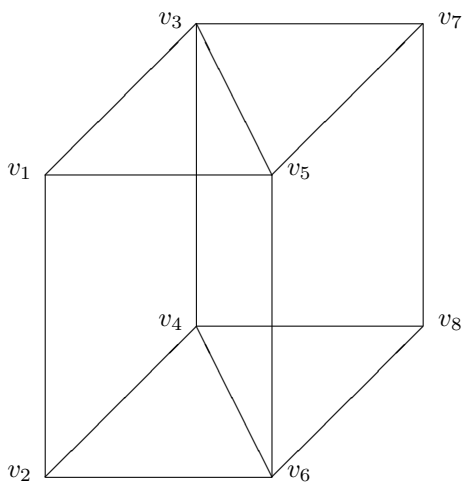


Figure 4.1: Intuition for the Vámos Matroid

Vámos matroid. Note that this means any qualified set that does not contain the dealer must include at least 3 participants.

The Vámos matroid is of interest for several reasons. Since any matroid on fewer than eight points is representable [20, p. 196], and the Vámos matroid is not representable [20], the Vámos matroid is a minimal example of a non-representable matroid. It is also the first known example of a matroid whose induced access structures do not admit ideal schemes [23]. The Vámos matroid provides the first known example of a matroid whose induced access structures have rates bounded away from 1, and the first examples of access structures with information rates strictly between 2/3 and 1 [1, 19].

The exact information rates of V_1 and V_6 are unknown. Martí-Farré and Padró showed that the rates must be at least 3/4 [19], while Beimel, Livne, and Padró used the Zhang-Yeung inequality to show that the information rates of V_1 and V_6 have upper bounds of 10/11 and 9/10 respectively [1] (Beimel et. al. refer to V_8 rather than V_1, but the two are isomorphic and V_1 is notationally more convenient for our purposes).

Here we improve the known upper bounds to 8/9 for V_1 and 17/19 for V_6, using non-Shannon inequalities found by Dougherty, Freiling, and Zeger [9]. The general method introduced here allows us to read off bounds for the information rate of V_6 directly from the coefficients of any non-Shannon inequality with certain properties, properties held by all four-variable non-Shannon inequalities of which we are aware.

4.2 The Usefulness of Non-Shannon Inequalities

To understand what we mean by "using" non-Shannon inequalities, recall that for an ideal scheme, the normalized entropy function h is the rank function of the matroid that induces the access structure for that scheme [15].

Assign the names A, B, C, D to Vámos pairs and consider the rank function of the Vámos matroid. Each Vámos pair has rank 2, and any union of three Vámos pairs has rank 4. Exactly one union of two Vámos pairs will have rank 4, and the others will have rank 3. If we choose AD to have rank 4, one can check that every non-Shannon inequality in Tables 3.2, 3.3, 3.4, and 3.5 will fail for the rank function of the Vámos matroid.

However, these non-Shannon inequalities must hold for any normalized entropy function obtained via secret sharing on V_6. We may thus obtain information about possible entropy functions by looking at these non-Shannon inequalities, which must be satisfied by entropy functions but not by the rank function of the Vamos matroid.

4.3 Properties of h for Schemes on V_1 and V_6

As in [1], for a fixed secret sharing scheme Σ on V_1 or V_6 we define

$$\lambda = \left(\max_{1 \le i \le 8} h(P_i) \right) - 1,$$

so that for each participant

$$h(v_i) \leq 1 + \lambda. \tag{4.1}$$

We note that by equation (2.2) the information rate of the scheme will then be

$$\rho(\Sigma) = \min_{1 \leq i \leq 8} \frac{1}{h(P_i)} = \frac{1}{1+\lambda}. \tag{4.2}$$

Immediately we have the following lemma.

Lemma 4.1. *For any pair X of participants, $h(X) \leq 2(1+\lambda)$.*

Proof. Let $X = \{p, q\}$. Then by the submodularity of h,

$$h(X) \leq h(\{p\}) + h(\{q\}) \leq (1+\lambda) + (1+\lambda). \qquad \square$$

We will be using Lemma 4.1 in the case where X is a Vámos pair.

Lemma 4.2. *Let X, Y be distinct Vámos pairs with XY a circuit. If the dealer is a member of Y, then*

(i) $h(Y|X) \leq 1 + \lambda$

(ii) $h(X|Y) \leq 1 + 2\lambda$.

Proof. Let $Y = \{s, t\}$ where s is the dealer, and let $X = \{p, q\}$.

(i) Since XY is a circuit containing the dealer, $X \cup \{t\}$ is a qualified set. Thus by Lemma 2.41, the submodularity of h, and equation (4.1),

$$h(Y|X) = h(\{t\}|X) \leq h(\{t\}) \leq 1 + \lambda.$$

(ii) The set $\{p, t\}$ is unqualified, as it is a set of size 2 that does not include the dealer. The set $X \cup \{t\}$ is qualified. Thus by Lemma 2.45,

$$h(\{p, t\}) + h(XY) + 1 \leq h(\{p\} \cup Y) + h(X \cup \{t\}).$$

Subtracting $h(Y)$ from both sides, rearranging, and using equation (4.1) gives us

$$\begin{aligned} h(X|Y) &\leq h(\{p\}|Y) + h(\{q\}|\{p,t\}) - 1 \\ &\leq h(\{p\}) + h(\{q\}) - 1 \\ &\leq 2(1+\lambda) - 1 \\ &= 1 + 2\lambda \end{aligned}$$

as desired.

□

Lemma 4.3. *Let X, Y be distinct Vámos pairs with XY a circuit. If neither X nor Y contains the dealer, then*

$$h(Y|X) \leq 1 + 3\lambda.$$

Proof. Let $Y = \{p, q\}$. Take r to be one of the two participants that is neither in XY nor in the Vámos pair of the dealer. Then we will have $X \cup \{r\} \notin \Gamma$, since adding the dealer to these three elements does not produce a circuit. We will have $X \cup \{p, r\}, X \cup \{q, r\} \in \Gamma$, since each of these is an independent set with four participants. Then by Lemma 2.45 we have

$$h(X \cup \{r\}) + h(XY \cup \{r\}) + 1 \leq h(X \cup \{p, r\}) + h(X \cup \{q, r\}).$$

Since $XY \notin \Gamma$, by Lemma 2.43 we have

$$h(XY) + 1 \leq h(XY \cup \{r\}).$$

We get the following from the submodularity of h:

$$\begin{aligned} h(X \cup \{p\}) &\leq h(X) + h(\{p\}) \\ h(X \cup \{p, r\}) &\leq h(X \cup \{p\}) + h(\{r\}) \\ h(X \cup \{q, r\}) &\leq h(X \cup \{r\}) + h(\{q\}). \end{aligned}$$

Finally, from equation (4.1),

$$\begin{aligned} h(\{p\}) &\leq 1 + \lambda \\ h(\{q\}) &\leq 1 + \lambda \\ h(\{r\}) &\leq 1 + \lambda. \end{aligned}$$

Adding the inequalities above, canceling terms, and writing as conditional entropy gives us the bound specified. □

Lemma 4.4. *Let X, Y be distinct Vámos pairs with XY independent. If the dealer is not a member of X, then*

$$2 \leq h(Y|X).$$

Proof. Case 1: Assume that the dealer is not a member of Y.

Let $Y = \{p, q\}$. Since XY is qualified but $X \cup \{p\}, X \cup \{q\}$ are not, by Lemma 2.43 we get the inequalities

$$\begin{aligned} 1 \leq& h(XY) - h(X \cup \{p\}) \\ 1 \leq& h(XY) - h(X \cup \{q\}). \end{aligned}$$

By the submodularity of h,

$$h(XY) + h(X) \leq h(X \cup \{p\}) + h(X \cup \{q\}).$$

Adding the above three inequalities, canceling terms, and rearranging gives the desired result.

Case 2: Assume that $Y = \{s, t\}$ where s is the dealer. Since XY is independent, $X \cup \{t\}$ is unqualified. Thus by Lemma 2.42

$$1 \leq h(XY) - h(X \cup \{t\}).$$

Let r be any participant not in XY. Then $X \cup \{r\}$ is also unqualified. Since $X \cup \{t, r\}$ is qualified, Lemma 2.44 tells us that

$$1 \leq h(X \cup \{t\}) - h(X).$$

Adding the above two inequalities gives the desired result. □

Although the previous lemma is stated in general terms, in practice it will only apply to the Vámos pairs $\{v_1, v_2\}$ and $\{v_7, v_8\}$, as any other two distinct Vámos pairs are dependent.

We will need one additional lemma to find bounds for the information rate of V_1. This lemma is also stated in general terms, although it will only apply to a few different choices for the Vámos pairs.

Lemma 4.5. *Let X, Y, Z be Vámos pairs with the dealer a member of Z. If XY, YZ are circuits and XZ is independent, then*

$$h(XY) + 3 \leq h(Y) + h(XZ).$$

Proof. Let $X = \{a, b\}, Y = \{p, q\}$, and $Z = \{s, t\}$ where s is the dealer. The sets $Y \cup \{a, t\}$ and $X \cup \{p, t\}$ are qualified, as each is an independent set of four elements. Since $\{a, p, t\}$ is unqualified, by Lemma 2.45 we have

$$h(XY \cup \{t\}) + h(\{a, p, t\}) + 1 \leq h(Y \cup \{a, t\}) + h(X \cup \{p, t\}).$$

To this we add the following inequalities, all consequences of the submodularity of h:

$$\begin{aligned} h(X \cup \{p,t\}) + h(\{a,t\}) &\leq h(\{a,p,t\}) + h(X \cup \{t\}) \\ h(Y \cup \{a,t\}) + h(\{a,q\}) &\leq h(Y \cup \{a\}) + h(\{a,q,t\}) \\ h(\{a,q,t\}) + h(\{a\}) &\leq h(\{a,q\}) + h(\{a,t\}) \\ h(Y \cup \{a\}) + h(\{p\}) &\leq h(Y) + h(\{a,p\}) \\ h(\{a,p\}) &\leq h(\{p\}) + h(\{a\}). \end{aligned}$$

After cancelling terms we obtain

$$h(XY \cup \{t\}) + 1 \leq h(Y) + h(X \cup \{t\}). \tag{4.3}$$

Since XY is a circuit which does not contain the dealer, XY is unqualified. As $XY \cup \{t\}$ is qualified, by Lemma 2.43

$$h(XY) + 1 \leq h(XY \cup \{t\})$$

which we add to (4.3) to obtain

$$h(XY) + 2 \leq h(Y) + h(X \cup \{t\}).$$

Finally, since XZ is independent, $X \cup \{t\}$ is unqualified. Thus by Lemma 2.42 we may substitute $h(XZ) - 1$ for $h(X \cup \{t\})$ in the previous inequality. Rearranging gives the desired result. □

4.4 A New Bound for the Information Rate of V_6

In [1] Beimel, Livne, and Padró found, by looking at the Zhang-Yeung non-Shannon inequality [33], that $1/9 \leq \lambda$ when v_6 is the dealer. Here we improve this bound by looking at a non-Shannon inequality from [9]. Let $A = \{v_1, v_2\}$, $B = \{v_3, v_4\}$, $C = \{v_5, v_6\}$, and $D = \{v_7, v_8\}$.

Theorem 4.6. *If the dealer is a member of C, then $2/17 \leq \lambda$.*

Proof. We use Dougherty, Freiling, and Zeger's inequality (i) from [9], which may be written

$$\begin{aligned}(\text{DFZi}) \qquad 0 \leq &-3h(A) - 5h(B) - 3h(C) + 8h(AB) \\ &+ 6h(AC) - 2h(AD) + 6h(BC) + 2h(BD) \\ &+ 2h(CD) - 9h(ABC) - 2h(BCD).\end{aligned}$$

Since $A, AB, BD \notin \Gamma$ and $ABC, BCD, AD \in \Gamma$, from Lemmas 2.43, 2.43, 4.4, and 2.44 respectively we obtain the following inequalities, which we add to (DFZi) with the indicated multiplicities:

$$\begin{aligned} 9[1 &\leq h(ABC) - h(AB)] \\ 2[1 &\leq h(BCD) - h(BD)] \\ 2[2 &\leq h(AD) - h(A)] \\ 1 &\leq h(AB) - h(A). \end{aligned}$$

After we cancel terms, the sum of inequalities yields

$$16 \leq -6h(A) - 5h(B) - 3h(C) + 6h(AC) + 6h(BC) + 2h(CD).$$

Rearranging, we obtain

$$16 \leq 6[h(AC) - h(A)] + 5[h(BC) - h(B)] + [h(BC) - h(C)] + 2[h(CD) - h(C)]$$

which may be further rewritten as

$$16 \leq 6h(C|A) + 5h(C|B) + h(B|C) + 2h(D|C).$$

Replacing each conditional normalized entropy by its upper bound from Lemma 4.2, we get

$$(4.4) \qquad 16 \leq 6(1+\lambda) + 5(1+\lambda) + (1+2\lambda) + 2(1+2\lambda).$$

This simplifies to

$$16 \leq 14 + 17\lambda \tag{4.5}$$

and we conclude that $2/17 \leq \lambda$. □

Corollary 4.7. *The information rate of V_6 is at most $\frac{17}{19}$.*

Proof. By Theorem 4.6 and equation (4.2), for any secret sharing scheme Σ on V_6 we have

$$\rho(\Sigma) = \frac{1}{1+\lambda} \leq \frac{17}{19}.$$

By the definition of information rate for an access structure,

$$\rho(V_6) \leq \frac{17}{19}.$$ □

4.5 From Non-Shannon Inequalities to Bounds on the Information Rate of V_6

Observe that the final steps of the proof of Theorem 4.6 are determined by the coefficients in the original non-Shannon inequality (DFZi). For example, the number of terms $(1 + 2\lambda)$ occurring in inequality (4.4) is equal to the absolute value of the coefficient on the term $h(C)$ in (DFZi). The method used in the proof of Theorem 4.6 allows one to read off a bound for λ directly from a non-Shannon inequality with certain properties, which we formulate using Definition 3.16. Let $A = \{v_1, v_2\}$, $B = \{v_3, v_4\}$, $C = \{v_5, v_6\}$, and $D = \{v_7, v_8\}$ as before, and recall the functions $\uparrow(\cdot)$ and $\downarrow(\cdot)$ from Definition 3.16.

Theorem 4.8. *Suppose the non-Shannon inequality*

$$0 \leq \sum_{X \subseteq \{A,B,C,D\}} C_X h(X) \tag{4.6}$$

has the following properties:

(i) *If* $|X| = 1$ *or* $|X| = 3$ *then* $C_X \leq 0$

(ii) $C_{AD} < 0$

(iii) *If* $|X| = 2$ *and* $X \neq \{A, D\}$ *then* $0 \leq C_X$

(iv) $C_{ABD} = C_{ACD} = C_{ABCD} = 0$

(v) *If* $|X| = 3$ *or* $X = \{A, B, C, D\}$ *then* $\downarrow (X) = 0$

(vi) $C_{AB} + C_{ABC} \leq 0$ *and* $C_{BD} + C_{BCD} \leq 0$.

Let Σ *be any secret sharing scheme on* V_6 *and let*

$$\lambda = \left(\max_{1 \leq i \leq 8} h(P_i) \right) - 1.$$

Then

$$0 < \frac{-C_{AD}}{-C_{ABC} - C_{BCD} - 2C_C} \leq \lambda.$$

We refrain from cancelling the negative signs in the fraction above because, by the hypotheses of Theorem 4.8, each negative sign is being applied to a non-positive term. We write the fraction this way so that the numerator and the denominator are each non-negative.

Since Theorem 4.8 provides a positive lower bound for λ, the following corollary says that the information rate of V_6 is bounded away from 1. The proof is similar to that of Corollary 4.7.

Corollary 4.9. *Given the same hypotheses as in Theorem 4.8,*

$$\rho(V_6) \leq \frac{-C_{ABC} - C_{BCD} - 2C_C}{-C_{ABC} - C_{BCD} - 2C_C - C_{AD}}.$$

To obtain the bound for λ given in Theorem 4.8 we will cancel out specific terms from non-Shannon inequality (4.6) by adding inequalities from earlier lemmas. As

we add inequalities, we introduce as many "ones" as possible on the smaller side of the inequality. We will be left with an expression that can be rearranged into pieces with nice upper bounds. For clarity we implement this process in four steps.

1. Cancel out all terms $h(ABC)$ and $h(BCD)$.

2. Cancel out the terms $h(X)$ for all subsets X such that $|X| = 2$ and X does not include the dealer. For the access structure V_6 these will be all terms $h(AB), h(AD)$, and $h(BD)$.

3. Rearrange terms and write as conditional entropies.

4. Apply the upper bounds found in Lemma 4.2 and simplify to obtain a lower bound for λ.

To prove the theorem we need to justify that we can indeed take each step outlined above, and that the bound for λ obtained in this manner will be as claimed. First we need to prove a couple of lemmas.

Lemma 4.10. *Given the hypotheses of Theorem 4.8, if* $|X| = 1$ *then*

$$\uparrow\ (X) = 0.$$

Proof. Let X be such that $|X| = 1$ and let $Y = \{A, B, C, D\} \setminus X$. Then by hypothesis (v) and the definition of $\uparrow(\cdot)$ and $\downarrow(\cdot)$,

$$\begin{aligned} 0 &= \downarrow (ABCD) \\ &= \uparrow (X) + \downarrow (Y). \end{aligned}$$

Since $\downarrow (Y) = 0$ by hypothesis (v), it follows that $\uparrow (X) = 0$ as well. □

Lemma 4.11. *Given the hypotheses of Theorem 4.8,*

$$C_{ABC} + C_{BCD} = C_A + C_B + C_C + C_D.$$

Proof. By hypothesis (v) and the definitions of $\uparrow(\cdot)$ and $\downarrow(\cdot)$,

$$\begin{aligned} 0 &= \downarrow(ACD) + \downarrow(ABD) \\ &= C_A + C_C + C_D + C_{AC} + C_{AD} + C_{CD} + C_{ACD} \\ &\quad + C_A + C_B + C_D + C_{AB} + C_{AD} + C_{BD} + C_{ABD}. \end{aligned}$$

To this we add the following equation, true by hypothesis (iv):

$$\begin{aligned} C_{ABC} + C_{BCD} &= C_{ABC} + C_{BCD} + C_{ABD} + C_{ABCD} \\ &\quad + C_{ACD} + C_{ABCD}. \end{aligned}$$

Simplifying the sum and applying Lemma 4.10 we get

$$\begin{aligned} 0 = \uparrow(A) + \uparrow(D) + C_A + C_B + C_C + C_D + -C_{ABC} - C_{BCD} \\ = C_A + C_B + C_C + C_D - C_{ABC} - C_{BCD}, \end{aligned}$$

which proves the lemma. □

Lemma 4.12. *Given the hypothesis of Theorem 4.8,*

$$C_{AD} + (C_{ABC} + C_{AB}) + (C_{BCD} + C_{BD}) = C_C.$$

Proof. The left hand side may be rearranged to

$$C_{AD} + C_{AB} + C_{BD} + (C_{ABC} + C_{BCD}),$$

which by Lemma 4.11 and hypothesis (iv) is equal to

$$C_{AD} + C_{AB} + C_{BD} + (C_A + C_B + C_C + C_D) + C_{ABD}.$$

By hypothesis (v) this simplifies to

$$C_C + \downarrow(ABD) = C_C.$$

□

Proof of Theorem 4.8. We walk through the steps outlined above in more detail.

Step 1: We eliminate all terms $h(ABC)$ and $h(BCD)$. By hypothesis (i), $-C_{ABC}$ and $-C_{BCD}$ are non-negative. By Lemma 2.43 we may add the inequalities

$$\begin{aligned} -C_{ABC}[1 &\leq h(ABC) - h(AB)] \\ -C_{BCD}[1 &\leq h(BCD) - h(BD)] \end{aligned}$$

to non-Shannon inequality 4.6. By hypothesis (iv) we obtain

$$\begin{aligned} -C_{ABC} - C_{BCD} \leq\ & C_A h(A) + C_B h(B) + C_C h(C) + C_D h(D) \\ & + (C_{AB} + C_{ABC}) h(AB) + C_{AC} h(AC) \\ & + C_{AD} h(AD) + C_{BC} h(BC) \\ & + (C_{BD} + C_{BCD}) h(BD) + C_{CD} h(CD). \end{aligned} \tag{4.7}$$

Step 2: In order to eliminate all terms $h(AB), h(AD)$, and $h(BD)$, we add three more inequalities to (4.7). The indicated multiplicities of these inequalities are guaranteed to be non-negative by hypotheses (ii) and (vi). By Lemma 4.4 we know

$$-C_{AD}[2 \leq h(AD) - h(A)].$$

By two applications of Lemma 2.44, with $Z = A \cup \{v_8\}$ and $Z = B \cup \{v_1\}$ respectively, we know

$$\begin{aligned} -(C_{AB} + C_{ABC})[1 \leq h(AB) - h(A)] \\ -(C_{BD} + C_{BCD})[1 \leq h(BD) - h(B)]. \end{aligned}$$

We have now added a total of

$$-C_{ABC} - C_{BCD} - 2C_{AD} - C_{AB} - C_{ABC} - C_{BD} - C_{BCD}$$

to the left-hand side of our original non-Shannon inequality (4.6). By application of Lemma 4.12, this simplifies to

$$-C_{ABC} - C_{BCD} - C_{AD} - C_C.$$

Letting

$$\begin{aligned} C'_A &= C_A + C_{AB} + C_{AD} + C_{ABC} \\ C'_B &= C_B + C_{BD} + C_{BCD} \end{aligned}$$

we now have the inequality

$$\begin{aligned} -C_{ABC} - C_{BCD} - C_{AD} - C_C \leq \quad & C'_A h(A) + C'_B h(B) + C_C h(C) + C_D h(D) \\ & + C_{AC} h(AC) + C_{BC} h(BC) + C_{CD} h(CD). \end{aligned} \tag{4.8}$$

Step 3: We need to know that we can rearrange all terms on the right-hand side of (4.8) into conditional entropies.

First, we group all terms $h(A)$ with terms $h(AC)$. By Lemma 4.10 and hypothesis (iv),

$$\begin{aligned} 0 = &\uparrow (A) \\ =&C_A + C_{AB} + C_{AC} + C_{AD} + C_{ABC} + C_{ABD} + C_{ACD} + C_{ABCD} \\ =&C'_A + C_{AC} + C_{ABD} + C_{ACD} + C_{ABCD} \\ =&C'_A + C_{AC}. \end{aligned}$$

Thus $C'_A = -C_{AC}$ and so

$$C'_A h(A) + C_{AC} h(AC) = C'_A h(A) - C'_A h(AC) = -C'_A h(C|A). \tag{4.9}$$

We note that $-C'_A$ is non-negative: By hypotheses (i), (ii), and (vi),

$$C'_A = C_A + C_{AD} + (C_{AB} + C_{ABC}) \leq 0.$$

Next we group all terms $h(B)$ with terms $h(BC)$ to obtain

$$C'_B h(B) + C_{BC} h(BC) = (C_{BC} + C'_B) h(BC) - C'_B h(C|B). \tag{4.10}$$

We know that $-C'_B$ is non-negative because by hypotheses (vi) and (i),

$$C'_B = C_B + (C_{BD} + C_{BCD}) \leq 0.$$

We also know that $(C_{BC} + C'_B)$ is non-negative, since by Lemma 4.10 and hypotheses (iv) and (vi),

$$\begin{aligned} 0 &= \uparrow (B) \\ &= C_{BC} + (C_B + C_{BD} + C_{BCD}) + (C_{AB} + C_{ABC}) \\ &\quad + C_{ABD} + C_{ABCD} \\ &\leq C_{BC} + C'_B. \end{aligned}$$

We can also associate all terms $h(D)$ to terms $h(CD)$. Rearranging, we get

$$C_D h(D) + C_{CD} h(CD) = (C_D + C_{CD}) h(CD) - C_D h(C|D). \tag{4.11}$$

We know that $-C_D$ is non-negative by hypothesis (i). By Lemma 4.10 and hypothesis (iv), (ii), and (vi),

$$\begin{aligned} 0 &= \uparrow (D) \\ &= C_D + C_{AD} + C_{BD} + C_{CD} \\ &\quad + C_{ABD} + C_{ACD} + C_{BCD} + C_{ABCD} \\ &= C_D + C_{CD} + C_{AD} + (C_{BD} + C_{BCD}) \\ &\leq C_D + C_{CD}, \end{aligned}$$

so we also know that $(C_D + C_{CD})$ is non-negative.

Finally, we show that we have enough $h(C)$ terms to group with the remaining terms $h(BC)$ and $h(CD)$. By hypothesis (v),

$$\begin{aligned} 0 &= \downarrow(BCD) \\ &= C_B + C_C + C_D + C_{BC} + C_{BD} + C_{CD} + C_{BCD} \\ &= C'_B + C_{BC} + C_C + C_D + C_{CD}. \end{aligned}$$

Thus

$$C_C = -(C'_B + C_{BC}) - (C_D + C_{CD})$$

and so we have

$$\begin{aligned} (4.12)\quad & C_C h(C) + (C_{BC} + C'_B)h(BC) + (C_D + C_{CD})h(CD) \\ & \qquad = (C'_B + C_{BC})h(B|C) + (C_D + C_{CD})h(D|C). \end{aligned}$$

Step 4: Applying the rearrangements in equations (4.9), (4.10), (4.11), and (4.12) to inequality (4.8), and applying the bounds found in Lemma 4.2, we get

$$\begin{aligned} -C_{ABC} - C_{BCD} - C_{AD} - C_C &\leq -C'_A h(C|A) - C'_B h(C|B) - C_D h(C|D) \\ &\quad + (C_{BC} + C'_B)h(B|C) + (C_{CD} + C_D)h(D|C) \\ &\leq -C'_A(1+\lambda) - C'_B(1+\lambda) - C_D(1+\lambda) \\ &\quad + (C_{BC} + C'_B)(1+2\lambda) + (C_{CD} + C_D)(1+2\lambda). \end{aligned}$$

The coefficient of $(1+\lambda)$ simplifies, by hypotheses (iv) and (v), to

$$\begin{aligned} -C'_A - C'_B - C_D &= (-C_A - C_{AD} - C_{AB} - C_{ABC}) \\ &\quad + (-C_B - C_{BD} - C_{BCD}) - C_D - C_{ABD} \\ &= -\downarrow(ABD) - C_{ABC} - C_{BCD} \\ &= -C_{ABC} - C_{BCD}. \end{aligned}$$

The coefficient of $(1+2\lambda)$ simplifies, by hypothesis (v), to

$$\begin{aligned}(C_{BC}+C'_B)+(C_{CD}+C_D) &= C_B+C_{BD}+C_{BCD}+C_{CD}+C_D+C_{BC}\\ &=\downarrow(BCD)-C_C\\ &=-C_C.\end{aligned}$$

Thus we obtain the much prettier inequality

$$-C_{ABC}-C_{BCD}-C_{AD}-C_C \leq (-C_{ABC}-C_{BCD})(1+\lambda)+(-C_C)(1+2\lambda).$$

Multiplying out terms and simplifying, we get

$$\begin{aligned}-C_{ABC}-C_{BCD}-C_{AD}-C_C \leq & -C_{ABC}-C_{BCD}-C_C\\ & +(-C_{ABC}-C_{BCD}-2C_C)\lambda\end{aligned}$$

and so

$$-C_{AD} \;\leq\; (-C_{ABC}-C_{BCD}-2C_C)\lambda.$$

By hypothesis (ii) we know that $-C_{AD}$ is strictly positive, and thus the coefficient of λ is strictly positive as well. We conclude that

$$0<\frac{-C_{AD}}{-C_{ABC}-C_{BCD}-2C_C}\leq\lambda. \qquad \square$$

4.6 A New Bound for the Information Rate of V_1

In [1], the Zhang-Yeung inequality was also used to show that $1/10 \leq \lambda$ when v_1 is the dealer. Here we improve that bound by starting with a sum of non-Shannon inequalities from [9], and proceeding in a manner similar to that used to prove the bound for V_6.

While we do not yet have a generalization of this method, computer optimization with MAPLE confirms that this is the best bound one can find given the Zhang-Yeung inequality and all non-Shannon inequalities in [9]. Again, let $A = \{v_1, v_2\}$, $B = \{v_3, v_4\}$, $C = \{v_5, v_6\}$, and $D = \{v_7, v_8\}$.

Theorem 4.13. *If the dealer is a member of A, then $1/8 \leq \lambda$.*

Proof. The non-Shannon inequality (iv) from [9] may be written as follows:

$$\begin{aligned}(\text{DFZiv}) \qquad 0 \leq & -h(A) - 5h(B) - 5h(C) + 6h(AB) \\ & + 6h(AC) - 2h(AD) + 8h(BC) + 2h(BD) \\ & + 2h(CD) - 9h(ABC) - 2h(BCD).\end{aligned}$$

After swapping the letters A and C, we may write inequality (vi) from [9] as follows:

$$\begin{aligned}(\text{DFZvi}) \qquad 0 \leq & -h(A) - 5h(B) - 5h(C) + 5h(AB) \\ & + 5h(AC) - 2h(AD) + 8h(BC) + 3h(BD) \\ & + 3h(CD) - 7h(ABC) - 4h(BCD).\end{aligned}$$

Summing (DFZiv) and (DFZvi) gives

$$\begin{aligned}(\text{DFZiv+vi}) \qquad 0 \leq & -2h(A) - 10h(B) - 10h(C) + 11h(AB) \\ & + 11h(AC) - 4h(AD) + 16h(BC) + 5h(BD) \\ & + 5h(CD) - 16h(ABC) - 6h(BCD).\end{aligned}$$

To (DFZiv+vi) we add the following inequalities, obtained from Lemmas 2.43, 2.44,

2.44, and 4.5 respectively, with the indicated multiplicities:

$$\begin{aligned} 16[1 &\leq h(ABC) - h(BC)] \\ 5[1 &\leq h(BCD) - h(BD)] \\ 1 &\leq h(BCD) - h(CD) \\ 4[3 &\leq h(C) + h(AD) - h(CD)]. \end{aligned}$$

After cancelling terms, simplifying, and rearranging, we obtain

$$\begin{aligned} 34 &\leq -2h(A) - 10h(B) - 10h(C) + 11h(AB) + 11h(AC) + 4h(C) \\ &= 10h(A|B) + 10h(A|C) + h(B|A) + h(C|A) + 4h(C). \end{aligned}$$

Applying the bounds in Lemmas 4.2 and 4.1, we get

$$34 \leq 10(1+\lambda) + 10(1+\lambda) + (1+2\lambda) + (1+2\lambda) + 4(2(1+\lambda)).$$

Simplifying gives $1/8 \leq \lambda$. □

Similarly to our results for V_6, we have the following.

Corollary 4.14. *The information rate of V_1 is at most $\frac{8}{9}$.*

4.7 Investigating the Bound on $\rho(V_6)$ via Other Non-Shannon Inequalities

The hypotheses of Theorem 4.8 are satisfied by the Zhang-Yeung inequality [33], the six non-Shannon inequalities given in [9], and the infinite sequences of non-Shannon inequalities for four variables given in [18] and [31], with A, B, C, D as assigned in the preceeding sections. Here we show that the bound presented in Section 4.4 is the greatest lower bound for λ that one can obtain by applying Theorem 4.8 to any of the aforementioned non-Shannon inequalities when A, B, C, D are each assigned to a distinct Vámos pair.

Different assignments of the letters A, B, C, D to the Vámos pairs will change at most the ranks of those subsets of $\{A, B, C, D\}$ that are the union of two Vámos pairs. We consider assignments of letters with $AD = \{v_1, v_2, v_7, v_8\}$, following the discussion in Section 4.2. Swapping A and D has no effect on the lower bound for λ obtained by use of Theorem 4.8. As one can check, swapping B and C in any of the non-Shannon inequalities under consideration will merely result in a possibly weaker bound than what we already have.

The coefficients and upward and downward sums of the six non-Shannon inequalities found by Dougherty, Freiling, and Zeger in [9] are shown in Tables 3.2 and 3.3. One can confirm from the table that each inequality satisfies the hypotheses of Theorem 4.8, and that the greatest lower bound for λ found by applying Theorem 4.8 to each of these six inequalities is $2/17$.

Table 3.4 shows the coefficients, upward sums, and downward sums for Inequality s, where s is a positive integer, in each of the two infinite sequences of inequalities found by Matúš [18]. As one may confirm from the table, for $s \geq 1$ Inequality s in either infinite sequence satisfies the hypotheses of Theorem 4.8, with the consequence that λ is bounded below by

$$\frac{s}{s^2 + 5s + 3}. \tag{4.13}$$

Using basic techniques of calculus one can confirm that (4.13) is maximized when $s = \sqrt{3}$. Since the inequalities are numbered by positive integers, we consider the resulting inequalities when $s = 1$ or $s = 2$. Inequality 1 in either sequence is the Zhang-Yeung inequality, and (4.13) tells us again that $1/9$ is a lower bound for λ. The inequalities in each sequence when $s = 2$ are already among those found in [9], and (4.13) again gives us the bound $2/17$.

The coefficients of inequality s in the infinite sequence found by Xu, Wang, and

Sun [31] are shown in Table 3.5. For $s = 1$ the inequality corresponds to a Shannon-type inequality, and for $s = 2$ the inequality is again the Zhang-Yeung inequality. For $s \geq 2$ inequality s satisfies the hypotheses of Theorem 4.8, as we confirmed with the aid of MAPLE due to the messy nature of the calculations. Theorem 4.8 then gives a lower bound for λ of

$$\frac{2^{(s-1)} - 1}{1 - 4 \cdot 2^{(s-1)} + \sqrt{2}S_+ - \sqrt{2}S_-}. \tag{4.14}$$

Using the MAPLE Optimization package, we find that, restricting to non-negative integer values, (4.14) is maximized when $s = 2$. At $s = 2$, (4.14) gives $1/9$, as we expect from the Zhang-Yeung inequality. Since (4.14) is maximized for $s = 2$, larger values of s will not produce any stronger lower bounds for λ than those we already have.

4.8 Optimization via MAPLE

We used computer optimization to verify that the bounds $\rho(V_6) \leq 17/19$ and $\rho(V_1) \leq 8/9$ are the best one can obtain under the combined constraints of the Shannon inequalities satisfied by the entropy function, the Zhang-Yeung inequality [33], and the six non-Shannon inequalities given in [9].

For each of the access structures V_1 and V_6 we wrote a short PERL program to generate all submodularity inequalities of the forms

$$h(X) + h(X \cup \{a, b\}) \leq h(X \cup \{a\}) + h(X \cup \{b\})$$

and, where appropriate,

$$h(X) + h(X \cup \{a, b\}) + 1 \leq h(X \cup \{a\}) + h(X \cup \{b\}),$$

that applied to the access structure in question. We entered these inequalities into

MAPLE along with all monotonicity inequalities of the form

$$h(P \setminus \{v_i\}) \leq h(P),$$

where P was the set of all non-dealer participants in the access structure and v_i ranged over P. By the discussion in Section 3.3, this provided MAPLE with a generating set of Shannon inequalities. We also entered into MAPLE the non-Shannon inequalities and bounds of the form

$$1 \leq h(v_i) \leq 1 + \lambda$$

for each non-dealer participant v_i.

When we used the function Minimize in the MAPLE Optimization package to minimize λ with the given constraints, the results agreed with the bounds found earlier in this chapter. We also used MAPLE to verify that these are the best bounds one can get under the additional constraints obtained by taking the same non-Shannon inequalities as above with all four assignments of A, B, C, D to $\{v_1, \ldots, v_8\}$ satisfying

$$\begin{aligned} \{A, D\} &= \{\{v_1, v_2\}, \{v_7, v_8\}\} \\ \{B, C\} &= \{\{v_3, v_4\}, \{v_5, v_6\}\}. \end{aligned}$$

The PERL programs and MAPLE commands used are given in the appendices to this chapter.

4.9 Appendix: PERL Program to Generate Submodularities for V1

```
#!/usr/bin/perl

# program to generate all the submodularity inequalities I need for the Vamos matroid, when 1 is the dealer
$dealer=1;

# end up with a pair
for ($i=1; $i<=7; $i++) {
    if($i!=$dealer){
for ($j=($i+1); $j<=8; $j++){
    if($j!=$dealer){
print "p".$i.$j."<=p".$i."+p".$j."\n";
    }}}}

# end up with a triple after adding 2 dif elts to a singleton
for ($i=1; $i<=6; $i++) { if($i!=$dealer){
    for ($j=$i+1; $j<=7; $j++){ if($j!=$dealer){
for($k=$j+1; $k<=8; $k++){ if($k!=$dealer){

    @ijk=sort($i,$j,$k);
    @ij=sort($i,$j); @ik=sort($i,$k); @jk=sort($j,$k);

    print "p".$ijk[0].$ijk[1].$ijk[2]."+p".$i."<=p".$ij[0].$ij[1]."+p".$ik[0].$ik[1]."\n";
    print "p".$ijk[0].$ijk[1].$ijk[2]."+p".$j."<=p".$ij[0].$ij[1]."+p".$jk[0].$jk[1]."\n";
    print "p".$ijk[0].$ijk[1].$ijk[2]."+p".$k."<=p".$ik[0].$ik[1]."+p".$jk[0].$jk[1]."\n";
   }}}}}}

# end up with a foursome after adding 2 dif elts to a double.
# no cases here where I want to add plus 1s, because two size three qualified sets cannot intersect in a pair.
for ($i=1; $i<=6; $i++) { if($i!=$dealer){
    for ($j=$i+1; $j<=7; $j++){ if($j!=$dealer){
for($k=$j+1; $k<=8; $k++){ if($k!=$dealer){
    for ($m=$k+1; $m<=8; $m++) { if($m!=$dealer){

    @ijkm=sort($i,$j,$k,$m);

    @ijk=sort($i,$j,$k); @ijm=sort($i,$j,$m); @ikm=sort($i,$k,$m); @jkm=sort($j,$k,$m);
```

```
    @ij=sort($i,$j); @ik=sort($i,$k); @im=sort($i,$m);
    @jk=sort($j,$k); @jm=sort($j,$m); @km=sort($k,$m);

    print "p".$ijkm[0].$ijkm[1].$ijkm[2].$ijkm[3]."+p".$ij[0].$ij[1]."<=p".$ijk[0].$ijk[1].$ijk[2]."+p".$ijm[0].$ijm[1].$ijm[2]."\n";
    print "p".$ijkm[0].$ijkm[1].$ijkm[2].$ijkm[3]."+p".$ik[0].$ik[1]."<=p".$ijk[0].$ijk[1].$ijk[2]."+p".$ikm[0].$ikm[1].$ikm[2]."\n";
    print "p".$ijkm[0].$ijkm[1].$ijkm[2].$ijkm[3]."+p".$im[0].$im[1]."<=p".$ijm[0].$ijm[1].$ijm[2]."+p".$ikm[0].$ikm[1].$ikm[2]."\n";
    print "p".$ijkm[0].$ijkm[1].$ijkm[2].$ijkm[3]."+p".$jk[0].$jk[1]."<=p".$ijk[0].$ijk[1].$ijk[2]."+p".$jkm[0].$jkm[1].$jkm[2]."\n";
    print "p".$ijkm[0].$ijkm[1].$ijkm[2].$ijkm[3]."+p".$jm[0].$jm[1]."<=p".$ijm[0].$ijm[1].$ijm[2]."+p".$jkm[0].$jkm[1].$jkm[2]."\n";
    print "p".$ijkm[0].$ijkm[1].$ijkm[2].$ijkm[3]."+p".$km[0].$km[1]."<=p".$ikm[0].$ikm[1].$ikm[2]."+p".$jkm[0].$jkm[1].$jkm[2]."\n";
 }}}}}}}}

# end up with a 5some after starting with 3 elts
for ($i=1; $i<=6; $i++) { if($i!=$dealer){
    for ($j=$i+1; $j<=7; $j++){ if($j!=$dealer){
        for($k=$j+1; $k<=8; $k++){ if($k!=$dealer){
            for ($m=1; $m<=8; $m++) { if($m!=$dealer && $m!=$i && $m!=$j && $m!=$k){
for ($n=$m+1; $n<=8; $n++) {if($n!=$dealer && $n!=$i && $n!= $j && $n!= $k && $n!=$m) {

    @five=sort($i,$j,$k,$m,$n);
    @three=($i,$j,$k);
    @four1=sort($i,$j,$k,$m);
    @four2=sort($i,$j,$k,$n);

    $five=join("",@five); $three=join("",@three); $four1=join("",@four1); $four2=join("",@four2);

# CHANGE THIS PART WHEN DEALER CHANGES
# this says if our threesome is already qualified, or if one of our foursomes is NOT qualified, we do not get the +1
    print "p".$five."+p".$three;
    if(!( ($three eq "234") || ($three eq "256") || ($four1 eq "3456") || ($four1 eq "3478") || ($four1 eq "5678") ||
  ($four2 eq"3456") || ($four2 eq "3478") || ($four2 eq "5678")))
    {
print "+1";
    }
    print "<=p".$four1."+p".$four2."\n";
    }}}}}}}}}

# end up with 6, start with 4
for ($h=1; $h<=5;$h++) { if($h!=$dealer){
    for ($i=$h+1; $i<=6; $i++) { if($i!=$dealer){
```

```
for ($j=$i+1; $j<=7; $j++){ if($j!=$dealer){
    for($k=$j+1; $k<=8; $k++){ if($k!=$dealer){
for ($m=1; $m<=8; $m++) { if($m!=$dealer && $m!=$h && $m!=$i && $m!=$j && $m!=$k){
    for ($n=$m+1; $n<=8; $n++) {if($n!=$dealer && $n!=$h && $n!=$i && $n!= $j && $n!= $k && $n!=$m) {

@top=sort($h,$i,$j,$k,$m,$n);
@bottom=($h,$i,$j,$k);
@side1=sort($h,$i,$j,$k,$m);
@side2=sort($h,$i,$j,$k,$n);

$top=join("",@top); $bottom=join("",@bottom); $side1=join("",@side1); $side2=join("",@side2);

print "p".$top."+p".$bottom;
# CHANGE WHEN DEALER CHANGES
# this says if our foursome at the bottom is unqualified, we get a plus 1.
if( $bottom eq "3456" || $bottom eq "3478" || $bottom eq "5678")
{
    print "+1";
}
print "<=p".$side1."+p".$side2."\n";
}}}}}}}}}}

# end up with 7, start with 5
for ($g=1; $g<=4;$g++) {if ($g!=$dealer){
    for ($h=$g+1; $h<=5;$h++) { if($h!=$dealer){
for ($i=$h+1; $i<=6; $i++) { if($i!=$dealer){
    for ($j=$i+1; $j<=7; $j++){ if($j!=$dealer){
for($k=$j+1; $k<=8; $k++){ if($k!=$dealer){
    for ($m=1; $m<=8; $m++) { if($m!=$dealer && $m!=$g && $m!=$h && $m!=$i && $m!=$j && $m!=$k){
for ($n=$m+1; $n<=8; $n++) {if($n!=$dealer && $n!=$g && $n!=$h && $n!=$i && $n!= $j && $n!= $k && $n!=$m) {

    @top=sort($g,$h,$i,$j,$k,$m,$n);
    @bottom=($g,$h,$i,$j,$k);
    @side1=sort($g,$h,$i,$j,$k,$m);
    @side2=sort($g,$h,$i,$j,$k,$n);

    $top=join("",@top); $bottom=join("",@bottom); $side1=join("",@side1); $side2=join("",@side2);

    print "p".$top."+p".$bottom;
```

```
    print "<=p".$side1."+p".$side2."\n";
    }}}}}}}}}}}}}
```

4.10 Appendix: MAPLE Commands for V1

```
Looking at Vamos matroid, 1 dealing.  Look for optimal value of lambda.
> with(Optimization):

Submodularities from MATHLAB/Vamos_1deals/submodularities.txt, generated by perl program
> submodularities := {<results of program>}:
> bounds := {1 <= p2, 1 <= p3, 1 <= p4, 1 <= p5, 1 <= p6, 1 <= p7, 1 <= p8, p2 <= 1+lamb,
             p3 <= 1+lamb, p4 <= 1+lamb, p5 <= 1+lamb, p6 <= 1+lamb, p7 <= 1+lamb, p8 <= 1+lamb};
> monotonicities := {p234567 <= p2345678, p234568 <= p2345678, p234578 <= p2345678, p234678 <= p2345678,
                     p235678 <= p2345678, p245678 <= p2345678, p345678 <= p2345678};
> ZY98 := {p2+1+2*p34+2*p56+(p278+1)+4*p23456+p345678 <= 3*p234+3*p256+3*p3456+p3478+p5678};
> Di := {3*(p2+1)+5*p34+3*p56+2*(p278+1)+9*p23456+2*p345678 <= 8*p234+6*p256+6*p3456+2*p3478+2*p5678};
> Dii := {2*(p2+1)+3*p34+5*p56+p78+2*(p278+1)+7*p23456+4*p345678 <= 5*p234+6*p256+6*p3456+3*p3478+4*p5678};
> Diii := {2*(p2+1)+7*p34+4*p56+2*(p278+1)+9*p23456+4*p345678 <= 8*p234+5*p256+9*p3456+3*p3478+3*p5678};
> Div := {p2+1+5*p34+5*p56+2*(p278+1)+9*p23456+2*p345678 <= 6*p234+6*p256+8*p3456+2*p3478+2*p5678};
> Dv := {p2+1+7*p34+4*p56+p78+2*(p278+1)+9*p23456+4*p345678 <= 7*p234+5*p256+9*p3456+4*p3478+3*p5678};
> Dvi := {p2+1+5*p34+5*p56+2*(p278+1)+7*p23456+4*p345678 <= 5*p234+5*p256+8*p3456+3*p3478+3*p5678};
> nonShannon := `union`(`union`(`union`(`union`(`union`(`union`(ZY98, Di), Dii), Diii), Div), Dv), Dvi);
> Minimize(lamb, `union`(`union`(`union`(nonShannon, submodularities), bounds), monotonicities), assume = nonnegative);
[0.124999999828726, [lamb = 0.124999999828726352, p2 = 1.12499999982872723, ...]]

With just ZY98 Don't get anything better
> Minimize(lamb, `union`(`union`(`union`(ZY98, submodularities), bounds), monotonicities), assume = nonnegative);
[0.124999999981862, [lamb = 0.124999999981861523, p2 = 1.12499999998186162, ...]]

Also consider A=78, D=12, B=34, C=56.
> ZYb := {p78+2*p34+2*p56+p278+1+4*p345678+p23456 <= 3*p3478+3*p5678+3*p3456+p234+p256};
> Dib := {3*p78+5*p34+3*p56+2*(p278+1)+9*p345678+2*p23456 <= 8*p3478+6*p5678+6*p3456+2*p234+2*p256};
> Diib := {2*p78+3*p34+5*p56+p2+1+2*(p278+1)+7*p345678+4*p23456 <= 5*p3478+6*p5678+6*p3456+3*p234+4*p256};
> Diiib := {2*p78+7*p34+4*p56+2*(p278+1)+9*p345678+4*p23456 <= 8*p3478+5*p5678+9*p3456+3*p234+3*p256};
> Divb := {p78+5*p34+5*p56+2*(p278+1)+9*p345678+2*p23456 <= 6*p3478+6*p5678+8*p3456+2*p234+2*p256};
> Dvb := {p78+7*p34+4*p56+p2+1+2*(p278+1)+9*p345678+4*p23456 <= 7*p3478+5*p5678+9*p3456+4*p234+3*p256};
> Dvib := {p78+5*p34+5*p56+2*(p278+1)+7*p345678+4*p23456 <= 5*p3478+5*p5678+8*p3456+3*p234+3*p256};
> ineqsb := `union`(`union`(`union`(`union`(`union`(`union`(`union`(`union`(`union`(`union`(submodularities,
```

```
            bounds), monotonicities), nonShannon), ZYb), Dib), Diib), Diiib), Divb), Dvb), Dvib);
> results := Minimize(lamb, ineqsb, assume = nonnegative);
Reassuringly, we still get lambda=1/8.
[0.124999999943304, [lamb = 0.124999999943303880, p2 = 1.12499999994330424, ...]]

Now include A=12 B=56 C=34 D=78.
ZY98, Div, and Dvi are symmetric in B and C so we don't need to do anything with them.
> Dic := {3*(p2+1)+5*p56+3*p34+2*(p278+1)+9*p23456+2*p345678 <= 8*p256+6*p234+6*p3456+2*p5678+2*p3478};
> Diic := {2*(p2+1)+3*p56+5*p34+p78+2*(p278+1)+7*p23456+4*p345678 <= 5*p256+6*p234+6*p3456+3*p5678+4*p3478};
> Diiic := {2*(p2+1)+7*p56+4*p34+2*(p278+1)+9*p23456+4*p345678 <= 8*p256+5*p234+9*p3456+3*p5678+3*p3478};
> Dvc := {p2+1+7*p56+4*p34+p78+2*(p278+1)+9*p23456+4*p345678 <= 7*p256+5*p234+9*p3456+4*p5678+3*p3478};
> ineqsc := `union`(`union`(`union`(`union`(ineqsb, Dic), Diic), Diiic), Dvc);
> results := Minimize(lamb, ineqsc, assume = nonnegative);
[0.124999998500857, [lamb = 0.124999998500857468, p2 = 1.12499999849102794, ...]]
phew, still getting 1/8

And one more:  A=78, B=56, C=34, D=12.
Again, ZY98, Div, and Dvi are symmetric in B and C so we don't need to do anything with them.
> Did := {3*p78+5*p56+3*p34+2*(p278+1)+9*p345678+2*p23456 <= 8*p5678+6*p3478+6*p3456+2*p256+2*p234};
> Diid := {2*p78+3*p56+5*p34+p2+1+2*(p278+1)+7*p345678+4*p23456 <= 5*p5678+6*p3478+6*p3456+3*p256+4*p234};
> Diiid := {2*p78+7*p56+4*p34+2*(p278+1)+9*p345678+4*p23456 <= 8*p5678+5*p3478+9*p3456+3*p256+3*p234};
> Dvd := {p78+7*p56+4*p34+p2+1+2*(p278+1)+9*p345678+4*p23456 <= 7*p5678+5*p3478+9*p3456+4*p256+3*p234};
> ineqsd := `union`(`union`(`union`(`union`(ineqsc, Did), Diid), Diiid), Dvd);
> Minimize(lamb, ineqsd, assume = nonnegative);
[0.124999999999219, [lamb = 0.124999999999219250, p2 = 1.12499999999921929...]]

Yup, still get 1/8.  So long as AD collectively are 1278, get 1/8 for lambda regardless of permutations of ABCD.
```

4.11 Appendix: PERL Program to Generate Submodularities for V6

```
#!/usr/bin/perl

# 11 Feb 2009 - originally 5 Nov 08
# program to generate all the submodularity inequalities I need for the Vamos matroid, when 6 is the dealer

# end up with a pair
$dealer=6;
```

```
for ($i=1; $i<=7; $i++) {
    if($i!=$dealer){
for ($j=($i+1); $j<=8; $j++){
    if($j!=$dealer){
print "p".$i.$j."<=p".$i."+p".$j."\n";
    }}}}

# end up with a triple after adding 2 dif elts to a singleton
for ($i=1; $i<=6; $i++) { if($i!=$dealer){
    for ($j=$i+1; $j<=7; $j++){ if($j!=$dealer){
for($k=$j+1; $k<=8; $k++){ if($k!=$dealer){

    @ijk=sort($i,$j,$k);
    @ij=sort($i,$j); @ik=sort($i,$k); @jk=sort($j,$k);

    print "p".$ijk[0].$ijk[1].$ijk[2]."+p".$i."<=p".$ij[0].$ij[1]."+p".$ik[0].$ik[1]."\n";
    print "p".$ijk[0].$ijk[1].$ijk[2]."+p".$j."<=p".$ij[0].$ij[1]."+p".$jk[0].$jk[1]."\n";
    print "p".$ijk[0].$ijk[1].$ijk[2]."+p".$k."<=p".$ik[0].$ik[1]."+p".$jk[0].$jk[1]."\n";
   }}}}}}

# end up with a foursome after adding 2 dif elts to a double.
# no cases here where I want to add plus 1s, because two size three qualified sets cannot intersect in a pair.
for ($i=1; $i<=6; $i++) { if($i!=$dealer){
    for ($j=$i+1; $j<=7; $j++){ if($j!=$dealer){
for($k=$j+1; $k<=8; $k++){ if($k!=$dealer){
    for ($m=$k+1; $m<=8; $m++) { if($m!=$dealer){

    @ijkm=sort($i,$j,$k,$m);

    @ijk=sort($i,$j,$k); @ijm=sort($i,$j,$m); @ikm=sort($i,$k,$m); @jkm=sort($j,$k,$m);

    @ij=sort($i,$j); @ik=sort($i,$k); @im=sort($i,$m);
    @jk=sort($j,$k); @jm=sort($j,$m); @km=sort($k,$m);

    print "p".$ijkm[0].$ijkm[1].$ijkm[2].$ijkm[3]."+p".$ij[0].$ij[1]."<=p".$ijk[0].$ijk[1].$ijk[2]."+p".$ijm[0].$ijm[1].$ijm[2]."\n";
    print "p".$ijkm[0].$ijkm[1].$ijkm[2].$ijkm[3]."+p".$ik[0].$ik[1]."<=p".$ijk[0].$ijk[1].$ijk[2]."+p".$ikm[0].$ikm[1].$ikm[2]."\n";
    print "p".$ijkm[0].$ijkm[1].$ijkm[2].$ijkm[3]."+p".$im[0].$im[1]."<=p".$ijm[0].$ijm[1].$ijm[2]."+p".$ikm[0].$ikm[1].$ikm[2]."\n";
    print "p".$ijkm[0].$ijkm[1].$ijkm[2].$ijkm[3]."+p".$jk[0].$jk[1]."<=p".$ijk[0].$ijk[1].$ijk[2]."+p".$jkm[0].$jkm[1].$jkm[2]."\n";
    print "p".$ijkm[0].$ijkm[1].$ijkm[2].$ijkm[3]."+p".$jm[0].$jm[1]."<=p".$ijm[0].$ijm[1].$ijm[2]."+p".$jkm[0].$jkm[1].$jkm[2]."\n";
```

```
    print "p".$ijkm[0].$ijkm[1].$ijkm[2].$ijkm[3]."+p".$km[0].$km[1]."<=p".$ikm[0].$ikm[1].$ikm[2]."+p".$jkm[0].$jkm[1].$jkm[2]."\n";
 }}}}}}}}

# end up with a 5some after starting with 3 elts
for ($i=1; $i<=6; $i++) { if($i!=$dealer){
    for ($j=$i+1; $j<=7; $j++){ if($j!=$dealer){
        for($k=$j+1; $k<=8; $k++){ if($k!=$dealer){
            for ($m=1; $m<=8; $m++) { if($m!=$dealer && $m!=$i && $m!=$j && $m!=$k){
for ($n=$m+1; $n<=8; $n++) {if($n!=$dealer && $n!=$i && $n!= $j && $n!= $k && $n!=$m) {

    @five=sort($i,$j,$k,$m,$n);
    @three=($i,$j,$k);
    @four1=sort($i,$j,$k,$m);
    @four2=sort($i,$j,$k,$n);

    $five=join("",@five); $three=join("",@three); $four1=join("",@four1); $four2=join("",@four2);

# CHANGE THIS PART WHEN DEALER CHANGES
# right now 6 is dealing
# this says if our threesome is already qualified, or if one of our foursomes is NOT qualified, we do not get the +1
    print "p".$five."+p".$three;
    if(!( ($three eq "125") || ($three eq "256") || ($three eq "578") || ($four1 eq "1234") || ($four1 eq "3478") ||
  ($four2 eq "1234") || ($four2 eq "3478") ))
    {
print "+1";
    }
    print "<=p".$four1."+p".$four2."\n";
    }}}}}}}}}

# end up with 6, start with 4
for ($h=1; $h<=5;$h++) { if($h!=$dealer){
    for ($i=$h+1; $i<=6; $i++) { if($i!=$dealer){
for ($j=$i+1; $j<=7; $j++){ if($j!=$dealer){
    for($k=$j+1; $k<=8; $k++){ if($k!=$dealer){
for ($m=1; $m<=8; $m++) { if($m!=$dealer && $m!=$h && $m!=$i && $m!=$j && $m!=$k){
    for ($n=$m+1; $n<=8; $n++) {if($n!=$dealer && $n!=$h && $n!=$i && $n!= $j && $n!= $k && $n!=$m) {

@top=sort($h,$i,$j,$k,$m,$n);
@bottom=($h,$i,$j,$k);
```

```
@side1=sort($h,$i,$j,$k,$m);
@side2=sort($h,$i,$j,$k,$n);

$top=join("",@top); $bottom=join("",@bottom); $side1=join("",@side1); $side2=join("",@side2);

print "p".$top."+p".$bottom;
# CHANGE WHEN DEALER CHANGES
# right now 6 is dealing
# this says if our foursome at the bottom is unqualified, we get a plus 1.
if( $bottom eq "1234" || $bottom eq "3478" )
{
    print "+1";
}
print "<=p".$side1."+p".$side2."\n";
}}}}}}}}}}}

# end up with 7, start with 5
for ($g=1; $g<=4;$g++) {if ($g!=$dealer){
    for ($h=$g+1; $h<=5;$h++) { if($h!=$dealer){
for ($i=$h+1; $i<=6; $i++) { if($i!=$dealer){
    for ($j=$i+1; $j<=7; $j++){ if($j!=$dealer){
for($k=$j+1; $k<=8; $k++){ if($k!=$dealer){
    for ($m=1; $m<=8; $m++) { if($m!=$dealer && $m!=$g && $m!=$h && $m!=$i && $m!=$j && $m!=$k){
for ($n=$m+1; $n<=8; $n++) {if($n!=$dealer && $n!=$g && $n!=$h && $n!=$i && $n!= $j && $n!= $k && $n!=$m) {

    @top=sort($g,$h,$i,$j,$k,$m,$n);
    @bottom=($g,$h,$i,$j,$k);
    @side1=sort($g,$h,$i,$j,$k,$m);
    @side2=sort($g,$h,$i,$j,$k,$n);

    $top=join("",@top); $bottom=join("",@bottom); $side1=join("",@side1); $side2=join("",@side2);

    print "p".$top."+p".$bottom;
    print "<=p".$side1."+p".$side2."\n";
    }}}}}}}}}}}}}
```

4.12 Appendix: MAPLE Commands for V6

```
6 is dealing
> with(Optimization):

submodularities created by the program generateSubmodularities.pl, in MATHLAB/Vamos_6deals
and edited using Emacs to be the right format for MAPLE
> submodularities := {<results of program>}:
> bounds := {1 <= p1, 1 <= p2, 1 <= p3, 1 <= p4, 1 <= p5, 1 <= p7, 1 <= p8, p1 <= 1+lamb, p2 <= 1+lamb,
             p3 <= 1+lamb, p4 <= 1+lamb, p5 <= 1+lamb, p7 <= 1+lamb, p8 <= 1+lamb};
> monotonicities := {p123457 <= p1234578, p123458 <= p1234578, p123478 <= p1234578, p123578 <= p1234578,
                     p124578 <= p1234578, p134578 <= p1234578, p234578 <= p1234578};

Minimize using Di with all permutations of letters
> Dia := {3*p12+5*p34+3*(p5+1)+2*p1278+9*p12345+2*p34578 <= 8*p1234+6*p125+6*p345+2*p3478+2*p578}:
> Dib := {3*p78+5*p34+3*(p5+1)+2*p1278+9*p34578+2*p12345 <= 8*p3478+6*p578+6*p345+2*p1234+2*p125}:
> Dic := {3*p12+5*(p5+1)+3*p34+2*p1278+9*p12345+2*p34578 <= 8*p125+6*p1234+6*p345+2*p578+2*p3478}:
> Did := {3*p78+5*(p5+1)+3*p34+2*p1278+9*p34578+2*p12345 <= 8*p578+6*p3478+6*p345+2*p1234+2*p125}:
> Di := `union`(`union`(`union`(Dia, Dib), Dic), Did):
> Minimize(lamb, `union`(`union`(`union`(Di, bounds), monotonicities), submodularities), assume = nonnegative);
[0.117647058787317, [p2478 = 4.23529411744071372, p4578 = 4.23529411785931753, ...]]

Minimize using all DFZ inequalities
> ZY98 := {p12+2*p34+2*(p5+1)+p1278+4*p12345+p34578 <= 3*p1234+3*p125+3*p345+p3478+p578};
> Dii := {2*p12+3*p34+5*(p5+1)+p78+2*p1278+7*p12345+4*p34578 <= 5*p1234+6*p125+6*p345+3*p3478+4*p578};
> Diii := {2*p12+7*p34+4*(p5+1)+2*p1278+9*p12345+4*p34578 <= 8*p1234+5*p125+9*p345+3*p3478+3*p578};
> Div := {p12+5*p34+5*(p5+1)+2*p1278+9*p12345+2*p34578 <= 6*p1234+6*p125+8*p345+2*p3478+2*p578};
> Dv := {p12+7*p34+4*(p5+1)+p78+2*p1278+9*p12345+4*p34578 <= 7*p1234+5*p125+9*p345+4*p3478+3*p578};
> Dvi := {p12+5*p34+5*(p5+1)+2*p1278+7*p12345+4*p34578 <= 5*p1234+5*p125+8*p345+3*p3478+3*p578};
> nonShannon := `union`(`union`(`union`(`union`(`union`(`union`(ZY98, Dia), Dii), Diii), Div), Dv), Dvi);
> Minimize(lamb, `union`(`union`(`union`(nonShannon, submodularities), bounds), monotonicities), assume = nonnegative);
[0.117647058714249, [lamb = 0.117647058714248562, p1 = 1.11764705871424774, ...]]

Minimize with just ZY98
> Minimize(lamb, `union`(`union`(`union`(ZY98, submodularities), bounds), monotonicities), assume = nonnegative);
[0.111111111031845, [lamb = 0.111111111031845178, p1 = 1.11111111103184590, ...]]

Trying different letter permutations for ABCD.
ineqs:=nonShannon union bounds union monotonicities union submodularities:
```

```
A=78 B=34 C=56 D=12
> bZY := {p78+2*p34+2*(p5+1)+p1278+4*p34578+p12345 <= 3*p3478+3*p578+3*p345+p1234+p125};
> bDi := {3*p78+5*p34+3*(p5+1)+2*p1278+9*p34578+2*p12345 <= 8*p3478+6*p578+6*p345+2*p1234+2*p125};
> bDii := {2*p78+3*p34+5*(p5+1)+p5+1+2*p1278+7*p34578+4*p12345 <= 5*p3478+6*p578+6*p345+3*p1234+4*p125};
> bDiii := {2*p78+7*p34+4*(p5+1)+2*p1278+9*p34578+4*p12345 <= 8*p3478+5*p578+9*p345+3*p1234+3*p125};
> bDiv := {p78+5*p34+5*(p5+1)+2*p1278+9*p34578+2*p12345 <= 6*p3478+6*p578+8*p345+2*p1234+2*p125};
> bDv := {p78+7*p34+4*(p5+1)+p5+1+2*p1278+9*p34578+4*p12345 <= 7*p3478+5*p578+9*p345+4*p1234+3*p125};
> bDvi := {p78+5*p34+5*(p5+1)+2*p1278+7*p34578+4*p12345 <= 5*p3478+5*p578+8*p345+3*p1234+3*p125};
> bineqs := `union`(`union`(`union`(`union`(`union`(`union`(`union`(ineqs, bZY), bDi), bDii), bDiii), bDiv), bDv), bDvi);
> Minimize(lamb, bineqs, assume = nonnegative);
[0.117647055681735, [lamb = 0.117647055681734766, p1 = 1.11764705568173550, ...]]

now A=12, B=56, C=34, D=78.  ZY98, Div, and Dvi are symmetric in B and C  so don't do anything with them.
> cDi := {3*p12+5*(p5+1)+3*p34+2*p1278+9*p12345+2*p34578 <= 8*p125+6*p1234+6*p345+2*p578+2*p3478};
> cDii := {2*p12+3*(p5+1)+5*p34+p78+2*p1278+7*p12345+4*p34578 <= 5*p125+6*p1234+6*p345+3*p578+4*p3478};
> cDiii := {2*p12+7*(p5+1)+4*p34+2*p1278+9*p12345+4*p34578 <= 8*p125+5*p1234+9*p345+3*p578+3*p3478};
> cDv := {p12+7*(p5+1)+4*p34+p78+2*p1278+9*p12345+4*p34578 <= 7*p125+5*p1234+9*p345+4*p578+3*p3478};
> cineqs := `union`(`union`(`union`(`union`(bineqs, cDi), cDii), cDiii), cDv);
> Minimize(lamb, cineqs, assume = nonnegative);
[0.117647055116658, [lamb = 0.117647055116658489, p1 = 1.11764705511665952, ...]]

one set left.  A=78, B=56, C=34, D=12.  Again, don't bother with ineqs symmetric in B and C.
> dDi := {3*p78+5*(p5+1)+3*p34+2*p1278+9*p34578+2*p12345 <= 8*p578+6*p3478+6*p345+2*p125+2*p1234};
> dDii := {2*p78+3*(p5+1)+5*p34+p12+2*p1278+7*p34578+4*p12345 <= 5*p578+6*p3478+6*p345+3*p125+4*p1234};
> dDiii := {2*p78+7*(p5+1)+4*p34+2*p1278+9*p34578+4*p12345 <= 8*p578+5*p3478+9*p345+3*p125+3*p1234};
> dDv := {p78+7*(p5+1)+4*p34+p12+2*p1278+9*p34578+4*p12345 <= 7*p578+5*p3478+9*p345+4*p125+3*p1234};
> dineqs := `union`(`union`(`union`(`union`(cineqs, dDi), dDii), dDiii), dDv);
> Minimize(lamb, dineqs, assume = nonnegative);
[0.117647058744904, [lamb = 0.117647058744903943, p1 = 1.11764705874490411, ...]]
```

CHAPTER 5

Information Rates of Minimal Non-Matroid-Related Access Structures

5.1 The King and n Pawns Access Structures

Definition 5.1. We define the *king and n pawns* access structure Γ_n for $n \geq 1$ on the set of participants $P_n = \{k, p_1, \ldots, p_n\}$ by

$$\Gamma_n = \{\{k, p_i\} | 1 \leq i \leq n\} \cup \{\{p_1, \ldots, p_n\}\}.$$

In Γ_n the king k and any one pawn p_i may reconstruct the secret, as may the set of all pawns. However, the king may not reconstruct the secret alone, nor may any proper subset of the pawns. This access structure may be pictured as in Figure 5.1.

The access structures Γ_n for $n \geq 3$, along with the three access structures

$$\{\{a, b\}, \{b, c\}, \{c, d\}\}$$

$$\{\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}\}$$

$$\{\{a, b\}, \{a, c\}, \{b, c, d\}\},$$

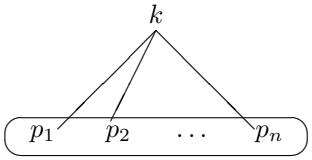


Figure 5.1: The King and n Pawns Access Structure

are the minor-minimal, non-matroid-related access structures [24]. Here we use "minor" in the sense of Definition 2.39. Any minor of one of these structures must therefore be matroid related, and any non-matroid related access structure must have one of these structures as a minor. Stinson [27] demonstrated that these last three access structures, as well as Γ_3, all have information rates of $\frac{2}{3}$. Here we find the exact information rates for all structures in the infinite class $\{\Gamma_n\}_{n\geq 2}$.

The main theorem of this chapter is the following.

Theorem 5.2. *For $n \geq 2$,*

$$\rho(\Gamma_n) = \frac{n-1}{2n-3}.$$

We will prove Theorem 5.2 by showing that $\frac{n-1}{2n-3}$ is both an upper and a lower bound for the information rate of Γ_n.

By Theorem 2.40, we have the following corollary.

Corollary 5.3. *Any access structure with the king and n pawns access structure as a minor has information rate at most $\frac{n-1}{2n-3}$.*

For the sake of readability, in the following we abbreviate $h(\{x_1, \ldots, x_i\})$ by $h(x_1 \ldots x_i)$.

5.2 Example: An Upper Bound for the Information Rate of Γ_5

The proof of the upper bound for general Γ_n will involve adding up a large collection of inequalities resulting from submodularity, +-submodularity, and monotonicity. In order to give the reader a picture of what is going on in the proof, we first provide a small example. We will work out the upper bound for $\rho(\Gamma_5)$, using visual representations of the inequalities involved. For the remainder of this section, fix an arbitrary secret sharing scheme realizing Γ_5.

Consider Figure 5.2. This figure may be thought of as showing four "pages" of a book whose spine is

$$\{p_1\} - \{p_1p_2\} - \{p_1 \dots p_3\} - \{p_1 \dots p_4\} - \{p_1 \dots p_5\} - \{kp_1 \dots p_5\}.$$

Each "page" represents a sum of inequalities.

When we add the Shannon inequalities represented by the diamonds in Figure 5.2, it can be seen from the picture that many terms will cancel out. For example, p_1p_2 is on the bottom of one diamond but on the side of another, so $h(p_1p_2)$ will cancel out when we add the corresponding inequalities. We will end up with

$$\begin{aligned} h(p_1) + 4h(kp_1 \dots p_5) + 4 \leq & h(kp_1 \dots p_4) + h(kp_1p_2p_3p_5) + h(kp_1p_2p_4p_5) \\ & + h(kp_1p_3p_4p_5) + h(p_1 \dots p_5). \end{aligned}$$

To this we further add the following inequalities, results of monotonicity:

$$\begin{aligned} h(kp_1p_2p_3p_5) \leq & h(kp_1 \dots p_5) \\ h(kp_1p_2p_4p_5) \leq & h(kp_1 \dots p_5) \\ h(kp_1p_3p_4p_5) \leq & h(kp_1 \dots p_5) \\ h(p_1 \dots p_5) \leq & h(kp_1 \dots p_5). \end{aligned}$$

Cancelling terms yields

$$h(p_1) + 4 \leq h(kp_1 \dots p_4). \tag{5.1}$$

Now consider Figure 5.3. This figure looks like four pages of a book with spine

$$\emptyset - \{k\} - \{kp_1\} - \{kp_1p_2\} - \{kp_1 \dots p_3\} - \{kp_1 \dots p_4\}.$$

Summing the inequalities represented by this figure yields

$$h(kp_1 \dots p_4) + 3 \leq h(p_1) + h(p_2) + h(p_3) + h(p_4) + h(k). \tag{5.2}$$

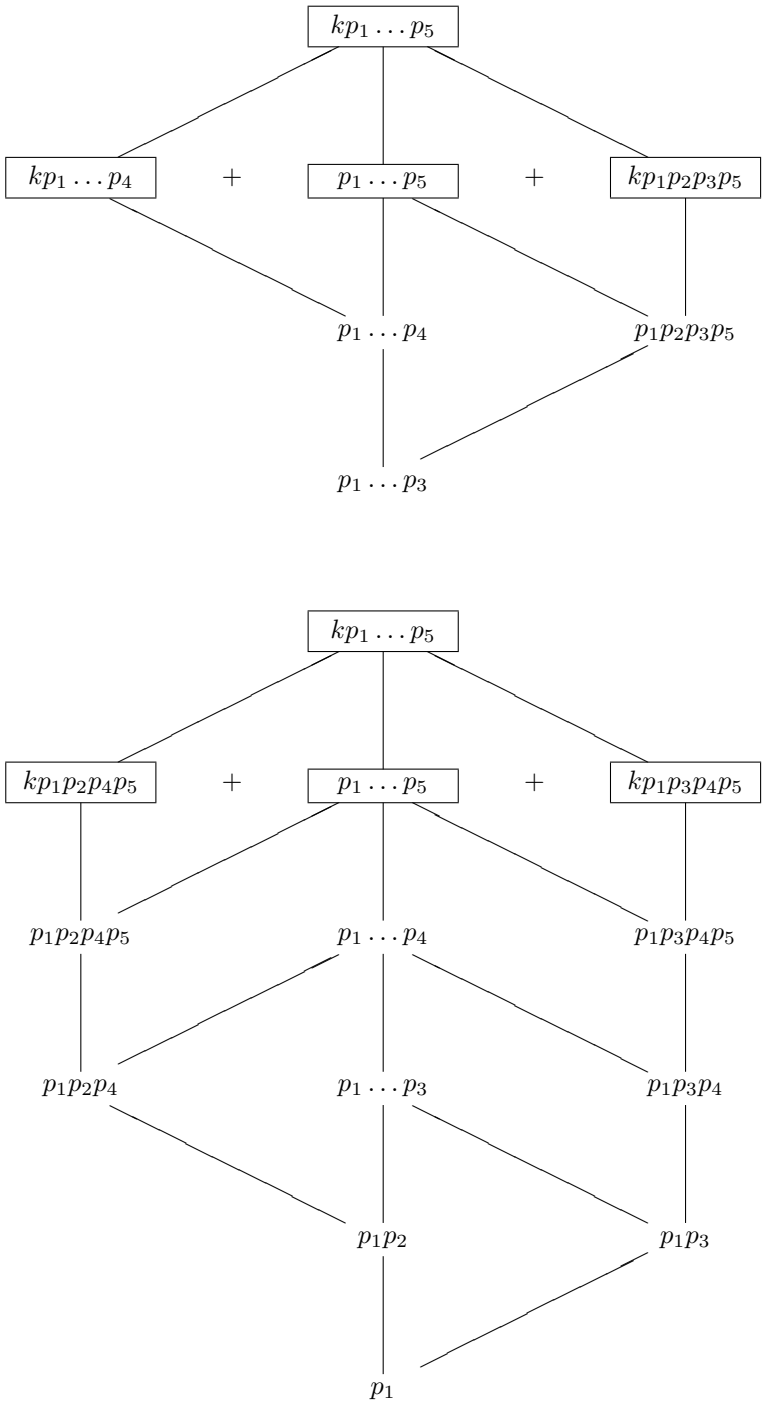


Figure 5.2: Downwards "Pages" of Inequalities

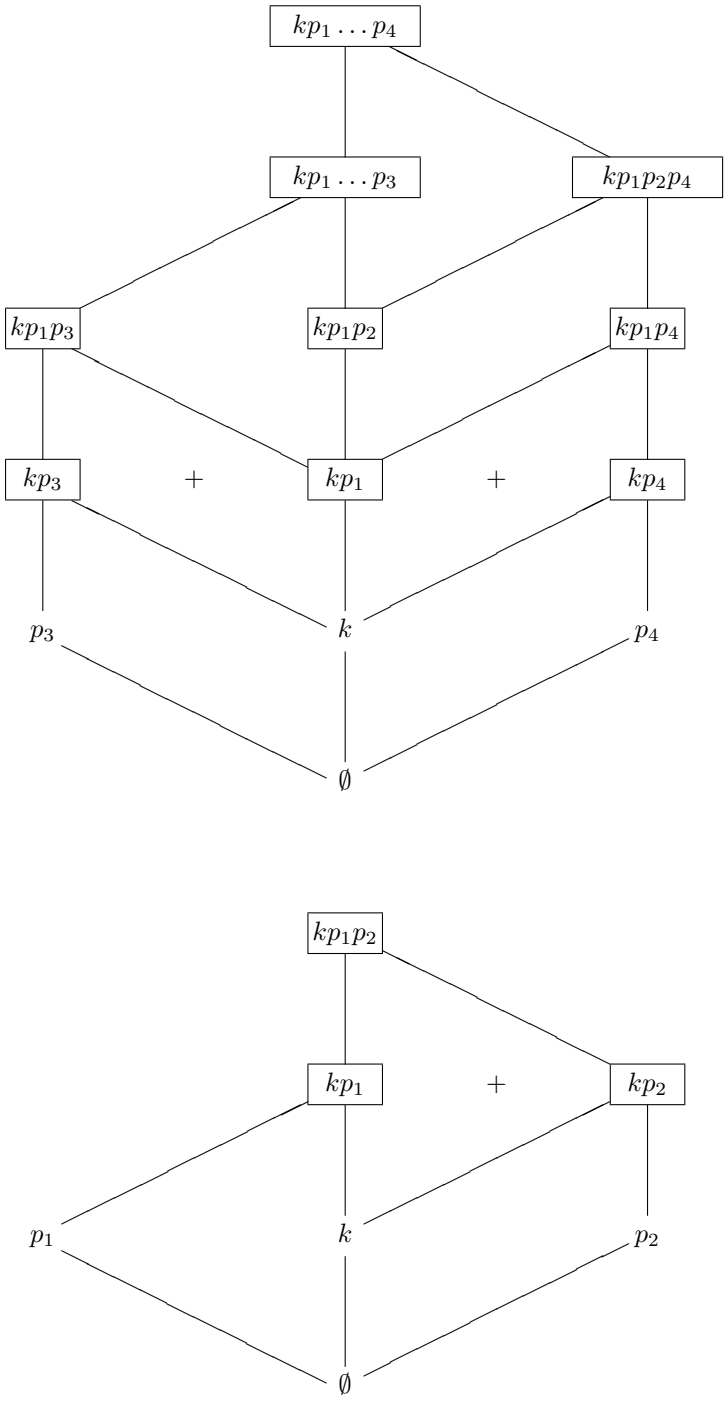


Figure 5.3: Upwards "Pages" of Inequalities

We observe that $\{kp_1 \dots p_4\}$ occurs on the top of a diamond in Figure 5.3, whereas in Figure 5.2 it occurred on the side of a diamond. Conversely, p_1 occurs on the side of diamond in Figure 5.3 but was on the bottom of a diamond in Figure 5.2. This makes inequalities 5.1 and 5.2 fit together quite nicely. Adding these two inequalities and cancelling terms gives

$$7 \leq h(p_2) + h(p_3) + h(p_4) + h(k),$$

which implies

$$7 \leq 4 \max_{p \in \{k, p_2, p_3, p_4\}} h(p).$$

This means at least one participant p must have normalized entropy at least $7/4$, hence information rate at most $4/7$. Since we started with an arbitrary secret sharing scheme for Γ_5, we conclude that

$$\rho(\Gamma_5) \leq \frac{4}{7}.$$

5.3 An Upper Bound for the Information Rate of Γ_n

For the general proof of the upper bound for the information rate of Γ_n, we need a couple of lemmas.

Lemma 5.4. *The function h satisfies*

$$h(p_1) + (n-1) \leq h(kp_1 \dots p_{n-1})$$

Proof. For any i in the range $2 \leq i \leq n$, we have (interpreting $p_{n+1}, \dots, p_n$ as an empty sequence)

$$\{p_1, \dots, p_n\} \in \Gamma,$$

$$\{k, p_1, \dots, p_{i-1}, p_{i+1}, \dots, p_n\} \in \Gamma$$

$$\{p_1, \dots, p_{i-1}, p_{i+1}, \dots, p_n\} \notin \Gamma.$$

By +-submodularity this produces the inequality

$$h(p_1 \dots p_{i-1}p_{i+1} \dots p_n) + h(kp_1 \dots p_n) + 1 \leq h(p_1 \dots p_n) + h(kp_1 \dots p_{i-1}p_{i+1} \dots p_n).$$

Adding the submodular inequality

$$h(p_1 \dots p_n) + h(p_1 \dots p_{i-1}) \leq h(p_1 \dots p_i) + h(p_1 \dots p_{i-1}p_{i+1} \dots p_n)$$

gives us

$$h(kp_1 \dots p_n) + h(p_1 \dots p_{i-1}) + 1 \leq h(kp_1 \dots p_{i-1}p_{i+1} \dots p_n) + h(p_1 \dots p_i). \tag{5.3}$$

Summing (5.3) over i from 2 to n, we get

$$(n-1)h(kp_1 \dots p_n) + \sum_{i=1}^{n-1} h(p_1 \dots p_i) + (n-1) \leq \sum_{i=2}^{n} h(kp_1 \dots p_{i-1}p_{i+1} \dots p_n) + \sum_{i=2}^{n} h(p_1 \dots p_i).$$

To this we add the monotonicities $h(kp_1 \dots p_{i-1}p_{i+1} \dots p_n) \leq h(kp_1 \dots p_n)$ for i from 2 to $n-1$ (not n) and $h(p_1 \dots p_n) \leq h(kp_1 \dots p_n)$. Cancelling terms gives us the desired result. □

We observe that inequality (5.3) corresponds to the sum of inequalities in one "page" of Figure 5.2. The final result of Lemma 5.4 corresponds to inequality (5.1) in the example we worked with Γ_5.

Similarly, inequality (5.4) in the next lemma corresponds to summing the inequalities in one "page" of Figure 5.3. The final result of the lemma corresponds to the sum of all "pages" from Figure 5.3 that contain a diamond resulting from +-submodularity.

Lemma 5.5. *The function h satisfies the inequality*

$$h(kp_1 \dots p_{n-1}) + (n-2) \leq h(kp_1) + \sum_{i=2}^{n-1} h(p_i).$$

Proof. For any i in the range $2 \leq i \leq n-1$, we have $\{kp_1\} \in \Gamma$, $\{kp_i\} \in \Gamma$, and $\{k\} \notin \Gamma$. By $+$-submodularity this produces the inequality

$$h(kp_1p_i) + h(k) + 1 \leq h(kp_1) + h(kp_i).$$

Adding this to the submodular inequalities

$$h(kp_i) \leq h(k) + h(p_i)$$

and

$$h(kp_1 \dots p_i) + h(kp_1) \leq h(kp_1 \dots p_{i-1}) + h(kp_1p_i)$$

gives us

$$h(kp_1 \dots p_i) + 1 \leq h(kp_1 \dots p_{i-1}) + h(p_i) \tag{5.4}$$

Summing (5.4) over i from 2 to $n-1$, we get

$$\sum_{i=2}^{n-1} h(kp_1 \dots p_i) + (n-2) \leq \sum_{i=1}^{n-2} h(kp_1 \dots p_i) + \sum_{i=2}^{n-1} h(p_i)$$

which simplifies to the desired result. □

If we were to draw visual representations for Γ_n as we did for Γ_5, Lemmas 5.5 and 5.4 would now have accounted for every "page" except the one corresponding to the submodularity

$$h(kp_1) \leq h(p_1) + h(k).$$

The proof of the theorem mainly consists of adding that last "page" to the results of the two lemmas, and interpreting the resulting inequality.

Theorem 5.6. *For the king and n-pawn access structure Γ_n*

$$\rho(\Gamma_n) \leq \frac{n-1}{2n-3}.$$

Proof. From Lemma 5.4 we have

$$h(p_1) + (n-1) \quad \leq \quad h(kp_1 \dots p_{n-1})$$

and from Lemma 5.5 we have

$$h(kp_1 \dots p_{n-1}) + (n-2) \quad \leq \quad h(kp_1) + \sum_{i=2}^{n-1} h(p_i)$$

We add to these inequalities the submodularity

$$h(kp_1) \quad \leq \quad h(p_1) + h(k)$$

to obtain

$$(2n-3) \leq h(k) + \sum_{i=2}^{n-1} h(p_i).$$

Since

$$h(k) + \sum_{i=2}^{n-1} h(p_i) \leq (n-1) \max_{p \in \{k, p_2 \dots p_{n-1}\}} h(p)$$

at least one participant p must satisfy

$$h(p) \geq \frac{2n-3}{n-1},$$

equivalently,

$$\rho(p) \leq \frac{n-1}{2n-3}.$$

Thus any secret sharing scheme for Γ_n must have information rate at most $\frac{n-1}{2n-3}$, and we conclude $\rho(\Gamma_n) \leq \frac{n-1}{2n-3}$. □

5.4 Schemes Realizing the Best Possible Information Rate for Γ_n

By the definition of information rate for an access structure, in order to prove a lower bound of $\frac{n-1}{2n-3}$ on $\rho(\Gamma_n)$ it suffices to construct a secret sharing scheme Σ for Γ_n realizing $\rho(\Sigma) = \frac{n-1}{2n-3}$. We begin by exhibiting two schemes for Γ_n, Σ_1 and Σ_2,

neither of which will attain the desired information rate. We will then take Σ to be a suitable weighted average of Σ_1 and Σ_2. For the constructions of Σ_1 and Σ_2 we assume the secret, s, is selected from the finite field $\mathbb{Z}_q$ where q is a prime greater than $(2n-1)$.

For the scheme Σ_1 we take a variant of an $(n, 2n-1)$ *threshold scheme* from [25], which we describe here. To share the secret s we choose uniformly at random a polynomial $f(x)$ over $\mathbb{Z}_q$ of degree at most $n-1$ with $f(0) = s$. The king then receives as his Σ_1-share the values $f(1), f(2), \ldots, f(n-1)$, and each p_i for $1 \leq i \leq n$ receives the value $f(n-1+i)$. That Σ_1 is indeed a secret sharing scheme for Γ_n follows from the discussion of threshold schemes in [25].

Lemma 5.7. *Each participant's Σ_1-share will occur with uniform distribution over the appropriate domain.*

Proof. First, we observe that any n equations of the form $f(x_1) = y_1$,$\ldots$, $f(x_n) = y_n$ for distinct values $x_1, \ldots, x_n$ are satisfied by exactly one polynomial f of degree at most $n-1$. For $m < n$ such equations $f(x_1) = y_1, \ldots, f(x_m) = y_m$, there will be exactly q^{n-m} polynomials that satisfy the set of equations. To see this, fix $x_{m+1}, \ldots, x_n$ distinct from each other and from the first m values of x. There are q^{n-m} ways to choose values $y_{m+1}, \ldots, y_n \in \mathbb{Z}_q$, and each choice of values will yield a unique polynomial.

We also observe that since the secret s was chosen uniformly, and the polynomial f of degree at most $n-1$ was chosen uniformly given the constraint $f(0) = s$, it follows that all polynomials f over $\mathbb{Z}_q$ of degree at most $n-1$ are equally likely to be used in Σ_1.

From the above observations, we see that any possible $(n-1)$-tuple of values for the king will be realized by q distinct polynomials. Since each polynomial is equally

likely, the king's Σ_1-share will be uniformly distributed over $\mathbb{Z}_q^{n-1}$. Similarly, any pawn's share will be realized by q^{n-1} distinct polynomials, each equally likely, and so a pawn's share will be uniformly distributed over $\mathbb{Z}_q$. □

The scheme Σ_2 is created using the decomposition method [27, 28], but the resulting scheme is simple enough to describe directly. We use a $(2, 2)$ threshold scheme and an (n, n) threshold scheme, also discussed in [27]. For the $(2, 2)$ threshold scheme, we distribute shares to members of the minimal qualified sets $\{k, p_i\}$ for $1 \leq i \leq n$, giving the king a random share $r \in \mathbb{Z}_q$, and giving each pawn the modular sum $r + s$. For the (n, n) threshold scheme, we distribute shares to members of the remaining minimal qualified set $\{p_1, \ldots, p_n\}$ by giving random values r_i, $1 \leq i \leq n-1$ to the first $n-1$ pawns, and giving to p_n the share

$$s + \sum_{i=1}^{n-1} r_i.$$

The king's Σ_2-share will be just his share from the $(2, 2)$ scheme. A pawn's Σ_2-share will consist of his shares from both the $(2, 2)$ and (n, n) schemes.

Any qualified set in Γ_n will be qualified in either the $(2, 2)$ or the (n, n) threshold scheme, and so will be qualified under Σ_2. Any set $X \subset P_n$ not in Γ_n will not be qualified in either of the threshold schemes being used for Σ_2. If all random numbers are chosen independently and uniformly, X will be unqualified under Σ_2. Furthermore, the Σ_2 shares for the king and each pawn will be uniformly distributed over $\mathbb{Z}_q$ and $(\mathbb{Z}_q)^2$, respectively.

We are now ready to construct the scheme Σ, which will allow us to share a secret that consists of $n-1$ secrets from $\mathbb{Z}_q$. To do this we share one secret using Σ_1, and $n-2$ secrets using different instantiations of Σ_2. We use uniformly and independently generated random numbers for each instantiation of a secret sharing scheme.

Theorem 5.8.

$$\rho(\Sigma) = \frac{n-1}{2n-3}.$$

Proof. The king's Σ-share will consist of $(n-1)+(n-2) = 2n-3$ shares from $\mathbb{Z}_q$. By Lemma 5.7 and the discussion regarding Σ_2 any Σ-share for the king will be equally likely, and so by Lemma 2.12,

$$\rho(k) = \frac{H(S)}{H(k)} = \frac{\log(q^{n-1})}{\log(q^{2n-3})} = \frac{n-1}{2n-3}.$$

Similarly, each pawn's Σ-share will consist of $1+2(n-2) = 2n-3$ shares from $\mathbb{Z}_q$, all possible Σ-shares having equal likelihood, and so we also have

$$\rho(p) = \frac{n-1}{2n-3}.$$

Thus

$$\rho(\Sigma) = \min\{\rho(k), \rho(p)\} = \frac{n-1}{2n-3}.$$

□

Theorem 5.9. *For the king and n-pawn access structure* Γ_n

$$\rho(\Gamma_n) \geq \frac{n-1}{2n-3}.$$

Proof. This follows immediately from Theorem 5.8 and the definition of information rate for an access structure. □

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] A. Beimel, N. Livne, C. Padró. Matroids Can Be Far From Ideal Secret Sharing. *Theory of Cryptography*, ed. Ran Canetti. New York: Springer, pp. 194-212, 2008.

[2] G. R. Blakley. Safeguarding Cryptographic Keys. *Proceedings of AFIPS National Computer Conference*, vol. 48, pp. 313-317, 1979.

[3] G. R. Blakley, C. Meadows. Security of Ramp Schemes. *Advances in Cryptology: Proceedings of CRYPTO 84*, eds. G. R. Blakley and D. C. Chaum. New York: Springer-Verlag, pp. 242-268, 1985.

[4] C. Blundo, A. De Santis, U. Vaccaro. On Secret Sharing Schemes. *Information Processing Letters*, vol. 65, pp. 25-32, 1998.

[5] C. Blundo, A. De Santis, R. De Simone, U. Vaccaro. Tight Bounds on the Information Rate of Secret Sharing Schemes. *Designs, Codes, and Cryptography*, vol. 11, no. 2, pp. 107-110, 1997.

[6] E. F. Brickell, D. M. Davenport. On the Classification of Ideal Secret Sharing Schemes. *Journal of Cryptology*, vol. 4, pp. 123-134, 1991.

[7] R. M. Capocelli, A. De Santis, L. Gargano, U. Vaccaro. On the Size of Shares for Secret Sharing Schemes. *Journal of Cryptology*, vol. 6, pp. 157-167, 1993.

[8] L. Csirmaz. The Size of a Share Must Be Large. *Journal of Cryptology*, vol. 10, n. 4, pp. 223-231, 1997.

[9] R. Dougherty, C. Freiling, K. Zeger. Six New Non-Shannon Information Inequalities. *2006 IEEE International Symposium on Information Theory*, pp. 233-236, 2006.

[10] W. Feller. *An Introduction to Probability Theory and its Applications.* New York : Wiley, 1968.

[11] S. Fujishige. Polymatroidal Dependence Structure of a Set of Random Variables. *Information and Control*, vol. 39, pp. 55-72, 1978.

[12] R. G. Gallager. *Information Theory and Reliable Communication.* New York: John Wiley and Sons, Inc., 1968.

[13] A. W. Ingleton. Representation of Matroids. *Combinatorial Mathematics and Its Applications*, ed. D. J. A. Welsh, pp. 149-167, 1971.

[14] E. D. Karnin, J. W. Greene, M. E. Hellman. On Secret Sharing Systems. *IEEE Transactions on Information Theory*, vol. 29, no. 1, pp. 35-41, 1983

[15] K. Kurosawa, K. Okada, K. Sakano, W. Ogata, S. Tsujii. Nonperfect secret sharing schemes and matroids. *EUROCRYPT '93*, pp. 126-141, 1994.

[16] K. Makarychev, Y. Makarychev. Conditionally Independent Random Variables. Information Theory ePrint Archive, 2005. http://arxiv.org/abs/cs/0510029

[17] F. Matúš. Conditional Independences among Four Random Variables III: Final Conclusion. *Combinatorics, Probability & Computing*, vol. 8, pp. 269-276, 1999.

[18] F. Matúš. Infinitely Many Information Inequalities. *IEEE International Symposium on Information Theory Proceedings*, pp. 41-44, 2007.

[19] J. Martí-Farré, C. Padró. On Secret Sharing Schemes, Matroids and Polymatroids. Cryptology ePrint Archive, Report 2006/077, 2006. http://eprint.iacr.org/.

[20] J. G. Oxley. *Matroid Theory*. New York: Oxford University Press, 1992.

[21] P. Paillier. On Ideal Non-Perfect Secret Sharing Schemes. *Proceedings of the 5th International Workshop on Security Protocols,* pp. 207-216, 1997.

[22] F. M. Reza. *An Introduction to Information Theory*. New York: McGraw-Hill Book Company, Inc., 1961.

[23] P. D. Seymour. On Secret-Sharing Matroids. *Journal of Combinatorial Theory, Series B*, vol. 56, no. 1, pp. 69-73, 1992.

[24] P.D. Seymour. A Forbidden Minor Characterization of Matroid Ports. *Quarterly Journal of Mathematics*, vol. 27, pp. 407-413, 1976.

[25] A. Shamir. How to Share a Secret. *Communications of the ACM*, vol. 22, n. 11, pp. 612-613, 1979.

[26] C. E. Shannon. A Mathematical Theory of Communication. *Bell System Technical Journal*, vol. 27, pp. 379-423, 623-656, 1948.

[27] D. R. Stinson. An Explication of Secret Sharing Schemes. *Designs, Codes and Cryptography*, vol. 2, n. 4, pp. 357-390, 1992.

[28] D. R. Stinson. Decomposition Constructions for Secret-Sharing Schemes. *IEEE Transactions on Information Theory*, vol. 40, no. 1, pp. 118-125, 1994.

[29] D. R. Stinson. *Cryptography Theory and Practice*. Boca Raton: Chapman & Hall/CRC, 2006.

[30] D. J. A. Welsh. *Matroid Theory*. London: Academic Press, 1976.

[31] W. Xu, J. Wang, J. Sun. A Projection Method for Derivation of Non-Shannon-Type Information Inequalities. arXiv.org Report 0804.4774, 2008. http://arxiv.org/abs/0804.4774.

[32] R. W. Yeung. *A First Course in Information Theory*. New York: Kluwer Academic / Plenum Publishers, 2002.

[33] Z. Zhang, R. W. Yeung. On Characterization of Entropy Function via Information Inequalities. *IEEE Transactions on Information Theory*, vol. 44, n. 4, pp. 1440-1452, 1998.