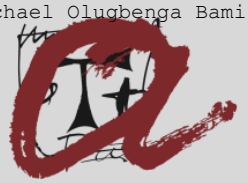
COMMON INFORMATION TECHNIQUES FOR THE STUDY OF MATROID REPRESENTATION AND SECRET SHARING SCHEMES

Michael Olugbenga Bamiloshin



UNIVERSITAT
ROVIRA i VIRGILI

Common Information Techniques For The Study Of Matroid Representation And Secret Sharing Schemes

---

Michael Olugbenga Bamiloshin

DOCTORAL THESIS
2021

UNIVERSITAT ROVIRA I VIRGILI
COMMON INFORMATION TECHNIQUES FOR THE STUDY OF MATROID REPRESENTATION AND SECRET SHARING SCHEMES
Michael Olugbenga Bamiloshin

UNIVERSITAT ROVIRA I VIRGILI
COMMON INFORMATION TECHNIQUES FOR THE STUDY OF MATROID REPRESENTATION AND SECRET SHARING SCHEMES
Michael Olugbenga Bamiloshin

UNIVERSITAT ROVIRA I VIRGILI
COMMON INFORMATION TECHNIQUES FOR THE STUDY OF MATROID REPRESENTATION AND SECRET SHARING SCHEMES
Michael Olugbenga Bamiloshin

Michael Olugbenga Bamiloshin

COMMON INFORMATION TECHNIQUES FOR THE STUDY OF MATROID REPRESENTATION AND SECRET SHARING SCHEMES

DOCTORAL THESIS

supervised by Dr. Oriol Farràs Ventura

Departament d'Enginyeria Informàtica i Matemàtiques

Tarragona, Catalonia, Spain
April 2021

UNIVERSITAT ROVIRA I VIRGILI
COMMON INFORMATION TECHNIQUES FOR THE STUDY OF MATROID REPRESENTATION AND SECRET SHARING SCHEMES
Michael Olugbenga Bamiloshin

UNIVERSITAT ROVIRA I VIRGILI

FAIG CONSTAR que aquest treball, titulat "Common Information Techniques For The Study Of Matroid Representation And Secret Sharing Schemes", que presenta Michael Olugbenga Bamiloshin per a l'obtenció del títol de Doctor, ha estat realitzat sota la meva direcció al Departament d'Enginyeria Informàtica i Matemàtiques d'aquesta universitat.

HAGO CONSTAR que el presente trabajo, titulado "Common Information Techniques For The Study Of Matroid Representation And Secret Sharing Schemes.", que presenta Michael Olugbenga Bamiloshin para la obtención del título de Doctor, ha sido realizado bajo mi dirección en el Departamento de Ingeniería Informática y Matemáticas de esta universidad.

I STATE that the present study, entitled "Common Information Techniques For The Study Of Matroid Representation And Secret Sharing Schemes", presented by Michael Olugbenga Bamiloshin for the award of the degree of Doctor, has been carried out under my supervision at the Department of Computer Science and Mathematics of this university.

Barcelona, 21-4-2021

El/s director/s de la tesi doctoral
El/los director/es de la tesis doctoral
Doctoral Thesis Supervisor/s

Oriol Farràs Ventura

UNIVERSITAT ROVIRA I VIRGILI
COMMON INFORMATION TECHNIQUES FOR THE STUDY OF MATROID REPRESENTATION AND SECRET SHARING SCHEMES
Michael Olugbenga Bamiloshin

The research presented in this thesis was carried out with funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 713679 and from the Universitat Rovira i Virgili (URV).

UNIVERSITAT ROVIRA I VIRGILI
COMMON INFORMATION TECHNIQUES FOR THE STUDY OF MATROID REPRESENTATION AND SECRET SHARING SCHEMES
Michael Olugbenga Bamiloshin

Acknowledgements

It is said that it takes a village to raise a child, and though a doctoral program doesn't take as much time as grooming a child from infancy to adulthood, the same principle applies. In light of this, and considering that this doctoral program is the concluding step in my academic studies, I owe a multitude of thanks to a "village" of people.

First for me will always be the One who has all things in His hands and through whom all things come: God. I am grateful for Your faithfulness and kindness not just during this program, but ever since my first breath.

My family will come next, for without their prayers and support, I would not even be here. Mum, Olubams, and Esther, thank you for it all.

Before coming to Tarragona in April 2018, I was in a city in Poland called Katowice. And before then, I was in L'Aquila, Italy. In these two places, I cultivated friendships that have kept me going at the toughest times. With Eze I learnt how to cook and we forged a bond that only a few will be able to outdo. With Alex, Madam Aida, Femi, and Evans, I found a group of people who inspire me with their perseverance (each of them is in a doctoral program somewhere). Pastor Shola and Sister Esther are always there for spiritual and moral guidance.

In some sense, I also would not be here had Professor Bruno Rubino not given me the opportunity to come to L'Aquila in September 2014. So I am grateful to him and the entire MathMods team.

Many thanks to every member of the CRISES research group, past and present, that I have had the chance to interact with; you all made this a safe space. Special thanks to Josep Domingo-Ferrer for his leadership of the group. Thanks also to *el jefe* Jesús "Txus" Manjón for..., well, for everything. Alberto was always ready to help with all my Daenerys-related problems. Special mention must also go to Romina and Ashneet for making Lab 131 more lively. The technical staff of DEIM were also really helpful to me. So also Dr Aïda Valls for her coordination of the department's doctoral program.

Though I ended up not being able to make use of it because of the pandemic, the Ferran Sunyer i Balaguer Foundation gave me a grant to undertake a 3-month research stay and I am thankful for that faith they put in me. In the same vein, I am also grateful to Professor László Csirmaz for agreeing to my doing this stay under his guidance at the Hungarian Academy of Science. It's a shame we could not make this happen.

My thanks cannot be complete if I have not mentioned my Church family here in Spain: The ICB family. Going from Tarragona to Barcelona every Sunday was not entirely

convenient but I never saw it as a problem because it was always a joy coming to Church. Serving with either the Frontlines or Media teams was always a highlight of my week. And to the ICB leadership headed by the Carranos, thank you for your leadership.

Thanks are definitely due to the COFUND leadership team: Bogdan, Oana, Paloma, Ana Benages and Sandra Flores, you all are very much appreciated. At every turn you were always willing to help. I am grateful. Thanks are also due to Marisol at the URV International Center. The Police appointments were easy because of you. Thank you.

Friends both home and abroad have also been really helpful, giving encouragement when it was needed. I would list all your names but that would take the whole space. Just know that I appreciate you all.

The results of this thesis were partly from a collaboration with some very talented researchers: Aner Ben-Efraim and Carles Padró. I learnt so much working with these people. Thank you for your mentorship.

Still on people I learned from, I would like to thank Guus P. Bollen. His work on algebraic matroids helped me refocus my work on the areas that really mattered. He was also very helpful when we asked him questions about some of the tools he used in his work (they are available on his Github repository which will be referenced a number of times in this thesis). I am grateful for your help. Same applies to Dillon Mayhew and Gordon F. Royle who made freely available to us the matroid database we so heavily relied on in this work. Many thanks to you both.

I would also like to thank my supervisors during my previous studies. O.A. Taiwo supervised me during my bachelors program, and Mieczysław Kula supervised my Masters thesis where he introduced me to the world of cryptography and secret sharing. Thank you both.

Sometimes, we save the best for last...

The success of a doctoral program depends largely on the two people most directly involved: the student and the supervisor. Any breakdown in the relationship between these two, any incompatibility, and the whole program might begin to fall apart.

I am grateful to have had Oriol Farràs as my supervisor. When I came newly to the university and people from the department would ask me who my supervisor was, once I told them it was Oriol, they would always tell me how lucky I was. It didn't take too long to see why this was true. Oriol is equal parts kind, gracious and knowledgeable. I am extremely grateful for your supervision, Oriol, and absolutely could not have done this program without your immense support and kindness. Your ability to guide and direct did me a lot of good. If I can be as kind, as gracious, as patient with others as

you were with me, then I will be confident that I learned all I ought to have learned from you. Words on paper are not enough to express my gratitude, but they will have to do for now. Thank you from the bottom of my heart.

UNIVERSITAT ROVIRA I VIRGILI
COMMON INFORMATION TECHNIQUES FOR THE STUDY OF MATROID REPRESENTATION AND SECRET SHARING SCHEMES
Michael Olugbenga Bamiloshin

UNIVERSITAT ROVIRA I VIRGILI

Abstract

Escola Tècnica Superior d'Enginyeria
Departament d'Enginyeria Informàtica i Matemàtiques

Doctor of Philosophy

by Michael Olugbenga Bamiloshin

The characterization of representable matroids is a longstanding open problem. This problem is connected to the characterization of access structures that admit ideal secret sharing schemes. In these schemes, the size of each share is equal to the size of the secret, which is an optimal situation. It is known that ports of entropic matroids are in correspondence with the access structures that admit ideal secret sharing schemes, while ports of linearly representable matroids are in correspondence with those that admit ideal linear schemes.

In this work, we develop new techinques to check representability properties that are based on different results of information theory such as the common information property and the Ahswelde-Körner lemma. With these techniques, we give a complete characterization of matroids on 8 points that admit folded linear (i.e., multilinear) representations, finding the smallest matroids that are not linearly representable but admit folded linear representations. Moreover, we determine the matroids on 8 points that are almost entropic, except for 3 of them. Furthering the work of Farràs, Kaced, Martín and Padró (IEEE Trans. Inf. Theory'20), we give lower bounds on the information ratio for secret sharing schemes for the ports of all matroids on 8 points and show a separation result for non-Ingleton-compliant sparse-paving matroids.

Combining these new techniques based on information theory with the Euclidean intersection property and other matroid intersection properties, we move further to 9-point matroids, finding new families of non-representable matroids that are Ingleton-compliant.

It is known that almost all matroids are not representable, and so almost all ports of matroids do not admit ideal linear schemes. However, it is not known if ports of matroids admit better schemes than general access structures. With the intention of shedding

some light on this question, we study matroids that are sparse paving, since this property is conjectured to be satisfied by almost all matroids. We show that ports of sparse-paving matroids admit schemes with sub-exponential share size. We also present exponential lower bounds for the information ratio of linear schemes for almost all matroid ports.

Contents

UNIVERSITAT ROVIRA I VIRGILI
COMMON INFORMATION TECHNIQUES FOR THE STUDY OF MATROID REPRESENTATION AND SECRET SHARING SCHEMES
Michael Olugbenga Bamiloshin

List of Figures

List of Tables

UNIVERSITAT ROVIRA I VIRGILI
COMMON INFORMATION TECHNIQUES FOR THE STUDY OF MATROID REPRESENTATION AND SECRET SHARING SCHEMES
Michael Olugbenga Bamiloshin

Outline of the Thesis

In this thesis, we study the problems of matroid representability and the search for lower bounds on the information ratio of secret sharing schemes. It is organized as follows.

We give a broad description of the goals and objectives of this thesis in Chapter 1, presenting an introduction to the areas of research we studied and the results we obtained.

In Chapter 2, we give formal definitions of concepts used. The first two sections cover concepts from information theory, the third is focused on matroids and polymatroids while the final section is devoted to secret sharing.

We go into our first contributions in Chapter 3 where we introduce the common information and Ahswelde-Körner information properties. We discuss these properties and also the linear programming (LP) techniques developed in this thesis.

In Chapter 4, we present our results on classification of matroids. Starting with matroids on 8 points, we look at folded linear and almost entropic classifications. We then move to matroids on 9 points where we present 3 new families of Ingleton-compliant non-linearly representable matroids. We also discuss connections between matroid intersection properties and end with a discussion on the state of matroids on up to 9 points with respect to algebraicity.

Along the same lines, we present results of our work in secret sharing in Chapter 5. First, we discuss the LP technique as applied to secret sharing and show bounds for matroid ports. We also give specific results for ports of sparse-paving matroids.

We present a summary of our results in Chapter 6 and discuss some interesting open problems as well.

In Appendix A, we present a table showing the algebraic status of every matroid in one of the families we introduced in Chapter 4.

Finally, in Appendix B, we present our computational results on secret sharing. In particular, we present bounds on σ for ports of matroids on 8 points, bounds on λ for ports of matroids on 9 points, and manually verifiable proofs for the bounds on a port of the Vámos matroid and also a port of the Tic-Tac-Toe matroid.

UNIVERSITAT ROVIRA I VIRGILI
COMMON INFORMATION TECHNIQUES FOR THE STUDY OF MATROID REPRESENTATION AND SECRET SHARING SCHEMES
Michael Olugbenga Bamiloshin

Dad, Mum, Olubams, CBams, and Estee, this one is for you. I hope I made you proud.

UNIVERSITAT ROVIRA I VIRGILI
COMMON INFORMATION TECHNIQUES FOR THE STUDY OF MATROID REPRESENTATION AND SECRET SHARING SCHEMES
Michael Olugbenga Bamiloshin

Chapter 1

Introduction

In this chapter we give a general idea of this thesis by introducing the research areas we focused on and the results we obtained.

1.1 Overview of the thesis

The characterization of representable matroids is a longstanding open problem in matroid theory. This problem is connected to the characterization of access structures that admit ideal secret sharing schemes. In such schemes, the size of each share is equal to the size of the secret, which is an optimal situation. It is known that ports of entropic matroids are in correspondence with the access structures that admit ideal secret sharing schemes, while ports of linearly representable matroids are in correspondence with those that admit ideal linear schemes.

Over time, different techniques have been applied to the study of the matroid representability problem, including using information and rank inequalities—like the Ingleton inequality [61]—and the forbidden minors characterization method.

The common information (CI) property and the copy lemma are two tools that have been used to derive non-Shannon-type linear information and rank inequalities. Similar to the copy lemma is the Ahswelde-Körner (AK) information property. It is known that the CI property is satisfied by linearly representable matroids while all almost entropic matroids satisfy the AK property. In this thesis, we present two new methods for the study of matroid representation properties. For folded-linear (i.e., multilinear) matroids, we develop a linear programming technique using the CI property, while for almost entropic matroids we develop an LP technique making use of the AK property.

We give a complete characterization of 8-point matroids with respect to folded linear representability—presenting the smallest folded-linear but non-linear matroids—and a near-complete characterization with respect to algebraicity and being almost entropic.

For matroids on 9-points and more, we needed supplementary tools to the ones we have just described. For this, we turned to matroid intersection properties: the Euclidean intersection property, Levi's intersection property, and the generalized Euclidean intersection property [3, 8, 9]. These are properties that are satisfied by linearly representable matroids. In this thesis, we develop recursive applications of these tools.

Using all the tools mentioned above, we found new non-representable matroids. We present a family of Ingleton-compliant matroids on 9 points having a configuration that prevents linear and folded-linear representability. Interestingly, like the Tic-Tac-Toe matroid, the duals of these matroids are not algebraic, but their own algebraicity is undetermined. We extend this family to include matroids on greater than 9 points. In addition, we present two other families of non folded-linear matroids.

The problem of representable matroids is one that carries over into the area of secret sharing in cryptography. Ideal access structures are ports of entropic matroids [31, 80] while ports of folded linear matroids admit ideal secret sharing schemes. Hence, determining which matroids satisfy which representation properties has implications for the study of efficiency measures in secret sharing.

Continuing with the work of Farràs et al. [50], we explore ports of matroids on 8 and 9 points. We give lower bounds on the information ratio of secret sharing schemes for the ports of all matroids on 8 points both for linear schemes and for general schemes. Furthermore, we also show a separation result on lower bounds on the information ratio of secret sharing schemes for ports of non-Ingleton-compliant sparse-paving matroids.

It is known that almost all matroids are not representable, and so almost all ports of matroids do not admit ideal linear schemes. However, it is not known if ports of matroids admit better schemes than general access structures. With the intention of shedding some light on this question, we study matroids that are sparse paving, since this property is conjectured to be satisfied by almost all matroids. We show that ports of sparse-paving matroids admit schemes with sub-exponential share size. We also present exponential lower bounds for the information ratio of linear schemes for almost all matroid ports.

1.2 Secret Sharing

In 1979, two researchers independently set out to answer two research questions that would birth an important area of cryptography. For George Blakley [26], it was the following (paraphrased): "*What's the best way to keep safe a cryptographic key? Do you make only a few copies and risk losing the whole information should these copies get missing? Or do you make several copies of it and risk letting it get to the wrong hands?*" Adi Shamir [102] on the other hand considered another question: "*Given eleven scientists working together on a secret project with a need to safeguard the documents in a cabinet, what is the smallest number of locks needed to keep the documents safe such that at least any six of the scientists together can open the cabinet? What is the smallest number of keys to the locks each scientist must carry?*" For both these researchers, the answer, though arrived at differently, was the same: *secret sharing schemes.*

The main idea of secret sharing is the following: *shares* are generated from the *secret* by an entity called the *dealer* and distributed to other entities typically called *participants* or *players* in such a way that only certain subsets of this larger group, called *authorized sets*, are able to put their shares together to recover the secret. The collection of all authorized subsets in a secret sharing scheme is called the *access structure* of the scheme and is denoted as Γ.

From being designed to solve the problem of secure information storage, secret sharing has grown to become a crucial primitive in such areas of cryptography as secure multi-party computation (MPC) (see for example [23, 34, 35]) which is an area of cryptography that involves allowing multiple users perform computation on their inputs without any user's input being revealed to the other users. The input of each user is taken as a secret and then shared among users by means of an appropriate secret sharing scheme. Later, computations on the secrets are made over these shares. Other applications of secret sharing include attribute-based encryption, access control, threshold cryptography, and so on (see [13]).

A secret sharing scheme is said to be *unconditionally secure* if its security is not as a result of any computational assumptions. The secret sharing schemes we discuss in this thesis are of this kind. Secret sharing schemes in which subsets of participants are either authorized or *forbidden* (i.e., get no information about the secret in the information theoretic sense) are known as *perfect* schemes. Karnin, Greene and Hellman [69] showed that in every perfect secret sharing scheme, each participant must have a share whose size is at least that of the secret. Those in which participants get shares the same size as the secret are called *ideal* schemes. If a subset is authorized, then all its supersets are also authorized. This is the *monotonicity* property of access structures. Ito, Saito and Nishizeki [63] showed how to construct a secret sharing scheme for any monotone increasing family of subsets. Hence, every monotone increasing family of subsets is an access structure. If a set is authorized and all its proper subsets are forbidden, then such a set is called a *minimal authorized set*. Every access structure is completely characterized by its family of minimal authorized sets denoted $\min\Gamma$.

The Shamir and Blakley schemes are both *threshold* secret sharing schemes. That is, the access structure Γ of these schemes consists of sets that are at least a given size. They are perfect, ideal and linear (i.e., sharing can be represented by a linear mapping over the field). In this thesis, we consider access structures that are of a more general nature.

Meaningful applications of secret sharing require efficient schemes. This efficiency is measured in a number of ways, from information ratio (which is a measure of the ratio between the share size and the secret size), to the share size in bits, and to sharing and reconstruction complexity.

General secret sharing constructions require shares of size $2^{O(n)}$ [5, 6, 24, 50, 63, 68, 75]. Recently, it was found that almost all access structures admit schemes with share size $2^{o(n)}$ [15]. However, whether this bound can be applied to all access structures is an open problem. There is still a huge gap between the best known upper and lower bounds. This is because the current best lower bound is still the $\Omega(n/\log n)$ bound obtained by Csirmaz [36].

The gap, however, is smaller for linear secret sharing schemes. These schemes are equivalent to *monotone span programs* [12, 30, 68]. Pitassi and Robere [97] showed that there are access structures that require $(\mathbb{F}_q, 1)$-linear schemes with information ratio $2^{\Omega(n)}$, and Babai et al. [7] showed that almost all access structures require $(\mathbb{F}_q, 1)$-linear schemes with information ratio $\Omega(2^{n/2-o(n)}/\sqrt{\log q})$.

The secret in the linear schemes above is a single field element. However, it is also possible to define the secret by a vector. Such schemes are known as *multi-linear* secret schemes in the literature [14, 25, 104]. Here, we call them folded-linear schemes. Using

these schemes it is sometimes possible to obtain better values of the information ratio, i.e., some access structures admit folded-linear schemes that are more efficient than linear schemes.

Characterization of families of access structures that admit efficient schemes is an interesting open problem. Of particular interest is the characterization of *ideal access structures*, that is, access structures that admit ideal secret sharing schemes. Such access structures have information ratio 1, which is the best possible case. No wonder then that these access structures have received considerable attention over the years (see, for example, [14, 17, 18, 21, 22, 31, 37, 47, 48, 50–52, 58, 78, 80, 89, 93, 104]).

Brickell and Davenport [31] showed that ideal access structures are ports of matroids, and Matúš [80] showed that they are indeed ports of entropic matroids. Hence, focusing on this characterization problem of ideal access structures, we move to matroid theory.

1.3 Matroids

Matroids were first introduced by Whitney [110] through an exploration of the link between the ideas of independence that came from linear algebra on the one hand and graph theory on the other [1]. In other words, matroids are a combinatorial object that abstract nicely the linear notions of independence.

There are a number of formal definitions of matroids that are essentially equivalent to each other. A constant presence in each of these definitions is a finite set of elements of the matroid that is called the *ground set* of the matroid. One formal definition is the following: Given a finite set Q and a nonnegative, integer-valued function r that is monotonic (i.e., for any $A \subseteq B \subseteq Q$, $r(A) \leq r(B)$), bounded by cardinality (i.e., $r(A) \leq |A|$ for any $A \subseteq Q$) and submodular (i.e, given any two sets $A, B \subseteq Q$, $r(A) + r(B) \geq r(A \cup B) + r(A \cap B)$), then the pair (Q, r) is a matroid with Q called its *ground set* and r its *rank function*.

A set is said to be *independent* if its rank equals its cardinality and *dependent* otherwise. Maximal independent sets of a matroid are called its *bases*. The bases of a matroid all have the same rank, and since the rank of every dependent set is the cardinality of its maximal independent subset, the rank of the matroid is the rank of its bases. The *closure* of a set B is the maximal superset of B having the same rank as B. A set is *closed* if it is its own closure. Closed sets are also sometimes referred to as *flats*. The minimal dependent sets of a matroid are called its *circuits*.

Matroids for which a matrix can be found where columns of the matrix are labelled by the elements of the matroid such that linear independence of submatrices is equivalent to independence of the labelling set of those submatrices are knonwn as *linearly* representable matroids if each element only labels a column, and *folded-linear* matroids if elements label a collection of columns. Folded-linear matroids have been called *multilinear* matroids in the literature. It is immediate that every linear matroid is also folded linear. Matroids can also be seen as a special case of *polymatroids* in the sense that the rank function of a polymatroid is not necessarily integer valued and that the rank of a

[1] For the sake of completeness, one might also mention the work by van der Waerden [107], though it came a couple of years after Whitney's work, as another introduction of matroids by exploring the link between the notion of algebraic independence and independence coming from linear algebra.

subset is not bounded by its cardinality. The definition of *linear* polymatroids follows that of linear matroids. The multiple of the rank function of a folded-linear matroid corresponds to that of some linear polymatroid. *Algebraic* matroids stem from van de Waerden's work [107]. The family of algebraic matroids contains all linear matroids. Some folded-linear matroids are algebraic and some algebraic matroids are folded-linear matroids, but the two classes do not coincide.

Determining whether a matroid belongs to any of the classes we have listed above is not an easy task. All matroids on up to 7 elements have been classified completely as they are all linearly representable. For matroids on 8 points and above, the work is still ongoing.

Tools for determining linear representability of a matroid include using excluded minors and the Ingleton inequality [61]. Mayhew and Royle [87] found that there are exactly 39 matroids on 8 points that are not Ingleton compliant and that any non-Ingleton-compliant 9-point matroid must have any one of these 39 as a minor. This result was later generalized to all sparse-paving non-Ingleton-compliant matroids on greater than 8 points [90].

Some other tools employed over the past 5 decades in the determination of a matroid's linear or algebraic representability have involved the same underlying concept: matroid extensions.

For linear matroids, these extension tools, also called intersection properties, include the Euclidean intersection property and the generalized Euclidean intersection property (see, for example, [3, 9]). These properties are satisfied by all linearly representable matroids. In the particular case of rank-4 matroids, these properties are equivalent to one another [9] and to the bundle condition [8], which is a configuration of lines in such matroids that prevent linear representability. The smallest matroids that do not satisfy these properties are the 39 matroids found in [87]. No such equivalence has been found for matroids of other ranks.

For a matroid to be algebraically representable, Ingleton and Main [62] showed that for any three lines that are pairwise—but not all—coplanar, the matroid must admit a proper (i.e., non-loop) extension such that the new element lies in the intersection of all three lines. Using this result, they were able to show the very first example of a non-algebraic matroid: the Vámos matroid. Lindstrom [74] later generalized this property and used it to show an infinite class of non-algebraic matroids. Using a different method, he also showed the existence of a different infinite class of non-algebraic matroids [73].

The *port* of a matroid at a point p_0 is the collection of all circuits containing p_0. The definition of matroid ports was first introduced by Lehman [71] in a context different from how it is used here. Brickell and Davenport [31] gave the first link between matroid theory and secret sharing by showing that ideal access structures are in fact determinied by matroids. That is, every ideal access structure is a matroid port. This result would go on to spur great research into the study of ideal access structures. Seymour [101] showed that the converse of the Brickell and Davenport result doesn't hold: not all matroid ports give rise to ideal access structures, using an example of a port of the Vámos matroid. Matroids that give rise to ideal access structures have also been referred to as partition-representable matroids [80].

Lower bounds on the information ratio of secret sharing schemes for matroid ports and also general access structures are usually obtained by the use of information inequalities.

1.4 Information Inequalities

The field of *information theory* came about as a result of Shannon's seminal paper [103]. Since then, information theory has grown to include applications in network coding, secret sharing, telecommunications, matroid theory, etc. The fundamental element in Shannon's work is the Shannon entropy which is a measure of the amount of uncertainty in a random variable. Using this, Shannon defined what are now called Shannon's *information measures* which consists of the entropy, *conditional entropy*, *mutual information*, and *conditional mutual information*, all of which are nonnegative.

A vector consisting of the Shannon entropies of all subsets of a finite set of random variables is called an *entropic vector*. Fujishige [55] observed that every entropic vector is the rank function of a polymatroid. *Entropic* polymatroids are those whose rank function is a multiple of an entropic vector. All linear polymatroids are entropic. A polymatroid that is the limit of a sequence of entropic polymatroids is called an *almost entropic* polymatroid. All algebraic matroids are almost entropic [82].

With these entities, one can go on to describe *information inequalities*, which are inequalities defined using entropies and that always hold for a sequence of random variables with joint distribution.

Shannon-type information inequalities are those information inequalities that can be expressed using only linear combinations (with nonnegative coefficients) of the conditional mutual information. Information inequalities that cannot be expressed in such a form are called *non-Shannon-type* information inequalities. The first example of a non-Shannon-type information inequality was presented by Zhang and Yeung [113]. Non-Shannon-type information inequalities are primarily derived using the *copy lemma* [114]. A similar technique is the *Ahswelde-Körner lemma* [1, 2]. Almost entropic matroids satisfy the Zhang-Yeung inequality and so do algebraic matroids.

Applications of information theory to secret sharing come via the use of information inequalilties in determining lower bounds on the information ratio of secret sharing schemes.

Rank inequalities, on the other hand, are inequalities satisfied by linear random variables. While all information inequalities are rank inequalities, the converse is not true. The first example to this effect was the rank inequality presented by Ingleton [61] which was shown to not be an information inequality by Hammer et al. [59]. They also showed that this inequality was derived by what is called the *common information* property, which is a property satisfied by linear random variables.

Most of the known rank inequalities have been derived using the common information property. However, some linear rank inequalities are derived by considering only fields with certain characteristic. For example, Peña and Sarria [94] derived linear rank inequalities satisfied by fields of characteristic 2, 3, or neither 2 nor 3. Such rank inequalities are said to be *characteristic dependent*.

1.5 LP Techniques for Secret Sharing

For finding lower bounds in secret sharing, the general idea is to use inequalities from information theory and then solve the linear programming problem defined on these inequalities. The first type of inequalities used were the Shannon-type information inequalities. A linear programming problem is defined using constraints derived from these inequalities with the solution giving a lower bound on the information ratio. This method, called the linear programming technique, was introduced by Capocelli et al.[33].

The notation κ was introduced in [78] to represent lower bounds on the information ratio obtained using Shannon-type information inequalities. The optimal information ratio, which is the infimum of the information ratios for all secret sharing schemes admitted by an access structure Γ is denoted σ for general schemes, and λ if only linear schemes are considered.

Using Shannon-type information inequalities, Csirmaz [36] found that there exists a family of access structures on n participants that require schemes with information ratio $\Omega(n/logn)$. This is the current best lower bound on the information ratio. Moreover, he also showed a limitation of this technique: the best lower bound on the information ratio that can be reached using only Shannon-type inequalities is at most n.

This was a rather crucial point since upper bounds on the information ratio are exponential [6, 24, 63] and so an improvement was needed if we were to close the gap between lower and upper bounds on the information ratio. This improvement came via using non-Shannon-type rank inequalities in the linear case and non-Shannon-type information inequalities in the general case [18]. Similar to the limitations of the Shannon-type information and rank inequalities, it was shown by Martin, Padró and Yang [79] that these non-Shannon-type inequalities can only prove, at best, polynomial lower bounds on the information ratio (Beimel and Orlov [19] proved a similar result for information inequalities on at most 5 variables).

Farràs et al. [50] later showed that instead of using these non-Shannon-type information and rank inequalities, it could be better to use the properties from which these inequalities are derived. In the case of rank inequalities, a common property they satisfy is the common information property, while for non-Shannon-type information inequalities, it is common to use the AK-information property. Applying constraints derived from these properties, better lower bounds have been found on the information ratio of secret sharing schemes [50].

1.6 Research Contributions

In this thesis, we studied the problems of matroid representability and the search for lower bounds on the information ratio of secret sharing schemes.

Starting with matroid representability, we developed the linear programming technique for secret sharing into a tool that can be applied in the study of this problem. In particular, we developed the LP technique using the common information (CI) property to find new non folded-linear matroids, and the Ahswelde-Körner (AK) information property to find matroids that are not almost entropic.

With these, we studied all matroids on 8 points. We found that the 39 matroids in [87] are not almost entropic by the AK property. From the five matroids on 8 points that are Ingleton-compliant but not linearly representable, we used the matrix representation of folded-linear matroids to prove that only two of them admit folded-linear representations. These folded-linear but non-linear matroids are the smallest such matroids. Doing this, we closed the classification of 8-point matroids with respect to folded-linear representability.

The matroid intersection properties of [9] are properties of linearly representable matorids. In their original definitions, however, they only deal with 1-step extensions of matroids. We developed these properties into tools that can be used in n-steps, for some positive integer n, to find matroids that might satisfy the properties at shallow depths but are not representable. These were particularly useful for us in our study of 9-point matroids.

From the matroid database provided by Royle and Mayhew [99], we selected matroids on 9 points with different ranks. We found new families of non-representable matroids using the intersection properties and also the LP techniques.

The first family we found, which we call the *TTT family*, consists of Ingleton-compliant sparse-paving rank-5 matroids. These matroids are non-linear matroids by the generalized Euclidean intersection property (GP) and non folded-linear matroids by the CI property. They break the Euclidean intersection property (EP) at depth 2 but satisfy the Ingleton-Main and Dress-Lovasz extension properties [28] at arbitrary depths. The duals of these matroids are not almost entropic by the AK property at depth 3. A prominent member of the TTT family is the Tic-Tac-Toe matroid. While Bollen [28] mentions 14 matroids he determined to be like the Tic-Tac-Toe matroid (though he doesn't identify them), we found 171 such matroids. An exhaustive search proved that there are no other rank-5 9-point matroids with this property.

The second family we found consists of some Ingleton-compliant non sparse-paving rank-5 matroids. Similar to the TTT family, matroids in this family are non-linear by 1-GP and non folded-linear by 1-CI. Their duals are also non almost-entropic matroids by the AK property at depth 3.

The third family of Ingleton-compliant non-linearly representable matroids we found consists of the first matroids we detected that satisfy the intersection properties at depth 1 but not at depth 2. In particular, they are 1-GP and 1-EP, but not 2-EP. We found many of them to be non folded-linear matroids by 2-CI.

Prior to now, techniques for finding lower bounds on the information ratio of secret sharing schemes involved using Shannon and non-Shannon-type information and rank inequalities. In this work, we continue with the innovation of [50] by using the properties through which these inequalities are derived. That is, we apply the CI and AK properties in the search for lower bounds.

Farràs et al. [50] looked at ports of some 8-point matroids and found bounds on both σ and λ. We extended this result by exploring ports of all 8-point matroids. Most of these matroids have the trivial bound on both σ and λ due to the fact that they are linearly representable. However, for the ports of the 39 matroids mentioned above, we obtained new lower bounds on σ for all of them and on λ for most of them.

We also looked at ports of some 9-point matroids. In particular, we looked at ports of rank-4 and rank-5 matroids due to the fact that matroids of rank less than 4 satisfy the CI property, and hence, have the trivial bound on both λ and σ. Also, we found a separation result for ports of sparse-paving matroids by showing that all sparse-paving non-Ingleton-compliant matroids have a lower bound of at least $4/3$ on λ and $9/8$ on σ. For the ports of the non Ingleton-compliant 9-point matroids we checked, the bounds on λ and σ were consistent with this separation result.

TTT matroids and matroids in the second family all had non-trivial bounds on λ. Considering that we are yet to find ports of any Ingleton-compliant 8-point matroid with a non-trivial bound, this makes the ports of these matroids to be one of the smallest such ports with non-trivial bounds on λ. Also, we were able to show that the $6/5$ bound on λ for one of the ports of the Tic-Tac-Toe matroid is tight by constructing a linear scheme for it. We also presented a manually verifiable proof of this result by listing all the inequalities involved in getting this bound.

We showed an application of the linear programming technique to the search for upper bounds on the coding capacities of networks. Studying the Vámos network, we derived the same upper bound on its coding capacity as obtained by Dougherty, Freiling and Zeger [42].

In addition to these computational bounds for matroid ports, we also found upper and lower bounds on the information ratio of secret sharing schemes for ports of sparse-paving matroids by other methods. We showed that the current best upper bounds on the information ratio that apply to almost all access structures [15] also apply to ports of sparse-paving matroids. That is, ports of sparse-paving matroids admit schemes with secrets in $\mathbb{F}_2$ and share size $2^{O(\sqrt{n}\log n)}$. Furthermore, we found new lower bounds on the information ratio of linear secret sharing schemes for these ports. In particular, we found that almost every matroid port requires 1-linear secret sharing schemes with information ratio $\Omega(2^{n/3-o(n)})$.

1.7 Publication List

Some of the results presented in this thesis are from the following publication.

1. M. Bamiloshin, A. Ben-Efraim, O. Farràs, and C. Padró. Common information, matroid representation, and secret sharing for matroid ports. *Designs, Codes, and Cryptography*, 89:143–166, 2021

In this thesis, we used the Gurobi$^{\text{TM}}$ optimizer for solving the linear programming problems, and the SageMath matroid package for specific matroid operations.

Codes relating to the results in this thesis are maintained at the following Github repositories:
`https://github.com/bmilosh/Common-Information-and-Matroid-Ports` and `https://github.com/bmilosh/TTT-And-Other-NonRepresentable-Matroids`.

UNIVERSITAT ROVIRA I VIRGILI
COMMON INFORMATION TECHNIQUES FOR THE STUDY OF MATROID REPRESENTATION AND SECRET SHARING SCHEMES
Michael Olugbenga Bamiloshin

Chapter 2

Preliminaries

In this chapter, we give a proper introduction of the concepts and structures that will be needed in the rest of this thesis.

2.1 Shannon's Information Measures

We start off with Shannon's information measures. They were introduced by Claude Shannon in his 1948 seminal paper [103] as part of the foundation of the field that is now called "information theory". An excellent resource for the topics covered here is Yeung's book on information theory [111]. Logarithms are taken to base 2.

Let X and Y be two random variables taking values in the alphabets $\mathcal{X}$ and $\mathcal{Y}$, respectively. The *probability distributions* of X and Y, respectively, are the nonnegative functions

$$p_X : \mathcal{X} \to \mathbb{R}_{\geq 0},$$

and

$$p_Y : \mathcal{Y} \to \mathbb{R}_{\geq 0}$$

whose values sum to 1. For brevity, we will write $p_X(x)$ as $p(x)$ for $x \in \mathcal{X}$, and $p_Y(y)$ as $p(y)$ for $y \in \mathcal{Y}$.

The *joint probability distribution* of X and Y is the nonnegative function

$$p_{XY} : \mathcal{X} \times \mathcal{Y} \to \mathbb{R}_{\geq 0}.$$

Also, the *conditional distribution* of the random variable X given that Y takes the value y is defined as

$$p_{X|Y=y}(x) = \frac{p_{XY}(x,y)}{p_Y(y)} = \frac{p(x,y)}{p(y)}$$

for $p(y) > 0$.

We will write the joint distribution as $p(x,y)$ and the conditional distribuion as $p(x|y)$.

Definition 2.1. The *entropy* of X is defined as

$$H(X) := -\sum_x p(x) \log p(x).$$

The entropy of a random variable X can be seen as the amount of bits needed to express X. It is also a measure of the amount of "uncertanty" in X. The entropy can be described as the fundamental measure of information, since, as we will soon show, the other information measures can be written as a combination of entropies.

Definition 2.2. The *joint entropy* $H(X,Y)$ of X and Y is defined as

$$H(X,Y) := -\sum_{x,y} p(x,y) \log p(x,y).$$

Definition 2.3. The *conditional entropy of X given Y* is defined as

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

The joint entropy of X and Y satisfies the equations

$$H(X,Y) = H(X) + H(Y|X) \quad \text{and} \quad H(X,Y) = H(Y) + H(X|Y),$$

which are both due to the fact that

$$p(x,y) = p(x) \cdot p(y|x) \quad \text{and} \quad p(x,y) = p(y) \cdot p(x|y).$$

Next, we define what is called the mutual information.

Definition 2.4. The *mutual information* $I(X;Y)$ of X and Y is defined as

$$I(X;Y) := \sum_{x,y} p(x,y) \log \frac{p(x,y)}{p(x)p(y)}.$$

The mutual information $I(X;Y)$ can be looked at as a measure of how much the two random variables X and Y have in common. Hence, it is symmetrical. The following relations all hold for the mutual information.

$$\begin{aligned} I(X;Y) &= H(X) - H(X|Y), \\ I(X;Y) &= H(Y) - H(Y|X), \\ I(X;Y) &= H(X) + H(Y) - H(X,Y). \end{aligned}$$

Figure 2.1 depicts how entropies and mutual information for two random variables are related using a venn diagram. Circle A represents the entropy of the random variable X while B represents that of the random variable Y. The joint entropy could be seen as the set $A \cup B$, the conditional entropy of Y on X as $B \setminus A$, the conditional entropy of X on Y as $A \setminus B$, and their mutual information as $A \cap B$.

If we introduce a third random variable Z taking values in the alphabet $\mathcal{Z}$ and with the nonnegative function

$$p_Z : \mathcal{Z} \to \mathbb{R}_{\geq 0}$$

as its probability distribution, we can define, analogous to the conditional entropy, the conditional mutual information as follows.

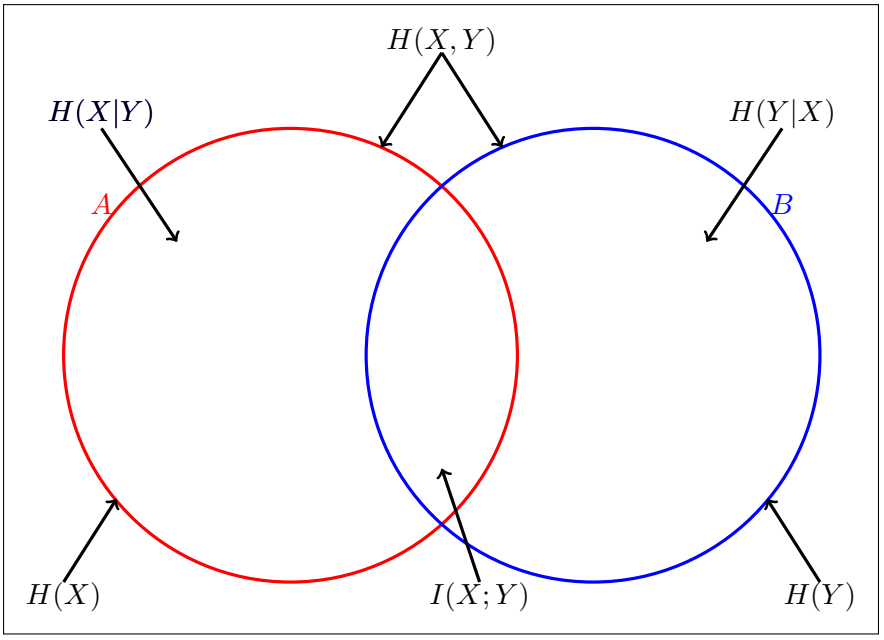


FIGURE 2.1: Relationship between entropies and mutual information for two random variables.

Definition 2.5. The *conditional mutual information* $I(X;Y|Z)$ of X and Y on Z is defined as

$$I(X;Y|Z) := \sum_{x,y,z} p(x,y,z) \log \frac{p(x,y|z)}{p(x|z)p(y|z)}.$$

The relations above for the mutual information also hold for the conditional mutual information if we condition each term in the relations on Z. We list them below.

$$\begin{aligned} I(X;Y|Z) &= H(X|Z) - H(X|Y,Z), \\ I(X;Y|Z) &= H(Y|Z) - H(Y|X,Z), \\ I(X;Y|Z) &= H(X|Z) + H(Y|Z) - H(X,Y|Z). \end{aligned}$$

It is important to note that, though we have given these definitions using only two or three random variables, the chain rule for information measures, which we will present in the following lemma, allows us to extend these definitions to any finite number of random variables. This will be useful when we talk about information inequalities in the next section.

Lemma 2.6. *Given jointly distributed random variables $X_1, \ldots, X_n, Y$ and Z, the* chain rule *for Shannon's information measures is given as:*

1. $H(X_1, \ldots, X_n) = \sum_{i=1}^{n} H(X_i|X_1, \ldots, X_{i-1})$ *(For entropy).*
2. $H(X_1, \ldots, X_n|Y) = \sum_{i=1}^{n} H(X_i|X_1, \ldots, X_{i-1}, Y)$ *(For conditional entropy).*
3. $I(X_1, \ldots, X_n; Y) = \sum_{i=1}^{n} I(X_i; Y|X_1, \ldots, X_{i-1})$ *(For mutual information).*
4. $I(X_1, \ldots, X_n; Y|Z) = \sum_{i=1}^{n} I(X_i; Y|X_1, \ldots, X_{i-1}, Z)$ *(For conditional mutual information).*

Also, considering the random variables in Lemma 2.6 and a set $A = \{1, \ldots, k\}$, we denote

$$H(X_A) := H(X_1, \ldots, X_k).$$

Remark 2.7. As Yeung [111] points out, the information measures we have defined are all special cases of the conditional mutual information. Let Φ represent a degenerate random variable (i.e., it takes a constant value with probability 1). The following relations hold for the conditional mutual information:

$$\begin{aligned} \text{if } Z = \Phi, \text{ then } I(X;Y|Z) &= I(X;Y), \\ \text{if } Y = X, \text{ then } I(X;Y|Z) &= H(X|Z), \\ \text{if } Y = X \text{ and } Z = \Phi, \text{ then } I(X;Y|Z) &= H(X). \end{aligned}$$

2.2 Information and Rank Inequalities

We can now go on to introduce some linear inequalities that are defined or expressed using these information measures.

Definition 2.8. Given a sequence of real numbers λ_i and sets $A_i \subseteq [n]$, a linear inequality of the form

$$\sum_{i=1}^{k} \lambda_i H(X_{A_i}) \geq 0 \tag{2.1}$$

that always holds for all jointly distributed random variables $X_1, \ldots, X_n$ is called an *information inequality*.

It is common to express information inequalities in a more compact form using combinations of the (conditional) mutual information and the conditional entropy, whenever appropriate. So for example, given three jointly distributed random variables X, Y, Z, some simple examples of information inequalities are as follows:

$$H(X) \geq 0 \tag{2.2}$$
$$H(X|Y) \geq 0 \tag{2.3}$$
$$I(X;Y) \geq 0 \tag{2.4}$$
$$I(X;Y|Z) \geq 0, \tag{2.5}$$

where 2.2 and 2.3 are nonnegative by definition, and 2.4 is nonnegative by what is called the *Jensen inequality*. For 2.5, observe that it can be expressed as

$$I(X;Y|Z) = H(X,Z) + H(Y,Z) - H(X,Y,Z) - H(Z),$$

which is nonnegative from the *submodularity* property of the entropy function. As we pointed out in Remark 2.7, each of equations 2.2– 2.4 is simply a consequence of Equation 2.5.

Definition 2.9. Let $X_1, \ldots, X_n, Y_1, \ldots, Y_n, Z_1, \ldots, Z_n$ be jointly distributed random variables. Any information inequality that can be written in the form

$$\sum_{i=1}^{n} \lambda_i I(X_i;Y_i|Z_i) \geq 0 \tag{2.6}$$

for some nonnegative λ_i is called a *Shannon-type information inequality.*

2.2.1 Non-Shannon-type Information Inequalities

Any information inequality that cannot be expressed in the form (2.6) above is referred to as a *non-Shannon-type information inequality.* Much of this work will be dedicated to non-Shannon-type information inequalities and their applications.

The first non-Shannon-type information inequality was derived by Zhang and Yeung [114].

Definition 2.10 (Zhang-Yeung's inequality)**.** Given any four jointly distributed random variables A, B, C, D the following inequality holds:

$$I(A;B) \leq 2I(A;B|C) + I(B;C|A) + I(A;C|B) + I(A;B|D) + I(C;D). \tag{2.7}$$

2.2.2 Rank Inequalities

Some information inequalities are such that they are only satisfied by linear variables or variables defined by linear mappings. We discuss these in this section.

Given a vector space $\mathcal{V}$ defined over a field $\mathbb{F}$ and subspaces $A_1, \ldots, A_n \subseteq \mathcal{V}$, by an abuse of notation, let $A_1, \ldots, A_n$ be the uniformly distributed random variables associated to these subspaces. For each subspace A_i of $\mathcal{V}$, we can express the entropy of its corresponding random variable as

$$H(A_i) = \dim(A_i) \cdot \log |\mathbb{F}|.$$

Definition 2.11. A linear inequality of the form (2.1) that always holds for all jointly distributed random variables defined over a vector space is called a *linear rank inequality.*

Linear rank inequalities are sometimes described as inequalities satisfied by ranks of vector subspaces. All information inequalities are also rank inequalities. The converse, however, is not true. The first example of a linear rank inequality that is not an information inequality was presented by Ingleton [61].

Definition 2.12 (Ingleton's Inequality)**.** Given a finite dimensional vector space $\mathcal{V}$, for any four subspaces A, B, C, D of $\mathcal{V}$, let S_A, S_B, S_C and S_D be random variables associated to these subspaces. Then the following holds:

$$I(S_A;S_B) \leq I(S_A;S_B|S_C) + I(S_A;S_B|S_D) + I(S_C;S_D). \tag{2.8}$$

Hammer et al. [59], proved that Ingleton's inequality is not an information inequality. This inequality finds application in a number of fields of study. But our focus in this work is its application to matroid theory, which was also the context in which Ingleton derived the inequality. He showed that for any four subsets of a linearly representable matroid, inequality (2.8) is always satisfied. Hammer et al. [59] showed that this is in fact the consequence of taking intersections of vector subspaces, something called the common information (an important ingredient of our work that we will look at in future chapters).

2.3 Matroids and Polymatroids

A detailed discussion on the subject of matroids can be found in Oxley's book on Matroid Theory [91].

Definition 2.13. A *polymatroid* is a pair (Q, r) where Q is a finite set and r is a real-valued function $r : \mathcal{P}(Q) \to \mathbb{R}$ satisfying the following conditions

(P1) $r(\emptyset) = 0$.

(P2) *Monotonicity*: $r(A) \leq r(B) \leq r(Q)$ for all $A \subseteq B \subseteq Q$.

(P3) *Submodularity*: $r(A) + r(B) \geq r(A \cup B) + r(A \cap B)$, for all $A \subseteq B \subseteq Q$.

The set Q is called the *ground set* of the polymatroid while r is called its *rank function*. Polymatroids in which the rank function only takes values in $\mathbb{Z}$ are called *integer* polymatroids.

If the pair (Q, r) is an integer polymatroid such that

$$r(A) \leq |A| \text{ for all } A \subseteq Q,$$

we call (Q, r) a *matroid*. While this definition makes use of the rank function of the matroid, there are other equivalent ways of defining matroids. We give another one below.

Definition 2.14. A *matroid* $\mathcal{M}$ is a pair $(Q, \mathcal{I})$ where Q is a finite set and $\mathcal{I}$ is a family of subsets of Q satisfying the following conditions

1. $\emptyset \in \mathcal{I}$.
2. If $B \in \mathcal{I}$ and $A \subseteq B$, then $A \in \mathcal{I}$.
3. If $A, B \in \mathcal{I}$ are such that $|A| < |B|$ then $\exists$ an element $b \in B \setminus A$ for which $A \cup \{b\} \in \mathcal{I}$.

Subsets of Q contained in $\mathcal{I}$ are called *independent* sets while subsets not in $\mathcal{I}$ are called *dependent* sets. Maximal elements of $\mathcal{I}$ are called *bases* of the matroid $\mathcal{M}$ while minimal dependent sets are called *circuits* of $\mathcal{M}$. A matroid is fully characterized by its bases (or equivalently, by its circuits). Every independent set A has the property that $r(A) = |A|$. On the other hand, the rank of a dependent set B is the size of the largest independent set it contains, i.e.,

$$r(B) = \max_{I \in \mathcal{I}, I \subseteq B} |I|.$$

And from this we see that the rank of a matroid $\mathcal{M}$ is simply the rank or cardinality of its bases. A matroid of rank 0 is called a *null* matroid. The *dual* of a matroid $\mathcal{M}$ is the matroid $\mathcal{M}^* = (Q, r^*)$ where $r^*(A) = |A| + r(Q \setminus A) - r(Q)$ for every $A \subseteq Q$.

The *closure* of a set $B \subseteq Q$ is the largest set $C \subseteq Q$ such that $C \supseteq B$ and $r(C) = r(B)$. A set $A \subseteq Q$ is called a *flat* or *closed set* if it is its own closure. In other words, if $r(B \cup x) > r(B)$ for every $x \in Q \setminus B$, then B is closed. Flats of rank 2 are called *lines*, while those of rank $r - 1$ are called *hyperplanes*. All circuits of $\mathcal{M}$ that are hyperplanes

are called *circuit-hyperplanes*. The process of transforming a circuit-hyperplane into a basis is a common one in matroid theory and is called a *relaxation* of the circuit-hyperplane. When a matroid is such that all its circuits have size r or $r+1$ it is called a *paving* matroid. If in addition its dual is paving, then we say the matroid is *sparse paving*. A matroid in which every set of size r is a basis is called a *uniform* matroid of rank r and is usually denoted $U_{r,n}$.

An element $e \in Q$ that is not contained in any basis of $\mathcal{M}$ is called a *loop*, while an element $e' \in Q$ contained in every basis is called a *coloop*. A matroid is said to be *simple* if it contains no loops, and *cosimple* if it has no coloops. Due to the fact that every matroid that is not a null matroid has at least one basis, no matroid has an element that is both a loop and coloop simultaneously. A matroid $\mathcal{M}$ is said to be *connected* if, for any two elements $e, e' \in Q$, there is a circuit of $\mathcal{M}$ containing them.

Consider two polymatroids $\mathcal{S}_1 = (Q, \mathcal{I}_1)$ and $\mathcal{S}_2 = (Q, \mathcal{I}_2)$ on the same ground set Q. The *sum* of $\mathcal{S}_1$ and $\mathcal{S}_2$ is given as

$$\mathcal{S} := \mathcal{S}_1 + \mathcal{S}_2 = (Q, \mathcal{I})$$

where a set $I \in Q$ is in $\mathcal{I}$ if and only if

$$I = I_1 \cup I_2 \text{ for some } I_1 \in \mathcal{I}_1 \text{ and } I_2 \in \mathcal{I}_2.$$

This is sometimes called the *union* of $\mathcal{S}_1$ and $\mathcal{S}_2$. However, if $\mathcal{S}_1$ and $\mathcal{S}_2$ are defined on different ground sets Q_1 and Q_2, respectively, then

$$\mathcal{S} := \mathcal{S}_1 \oplus \mathcal{S}_2 = (Q, \mathcal{I})$$

where $Q = Q_1 \cup Q_2$ and $I \in Q$ is in $\mathcal{I}$ if and only if

$$I = I_1 \cup I_2 \text{ for some } I_1 \in \mathcal{I}_1 \text{ and } I_2 \in \mathcal{I}_2,$$

is called the *direct sum* of $\mathcal{S}_1$ and $\mathcal{S}_2$. Observe that $\mathcal{S}$ is also a polymatroid in both cases. Also, given $g > 0$, $g\mathcal{S} = (Q, g \cdot r)$ is a polymatroid referred to as a *multiple* of $\mathcal{S}$.

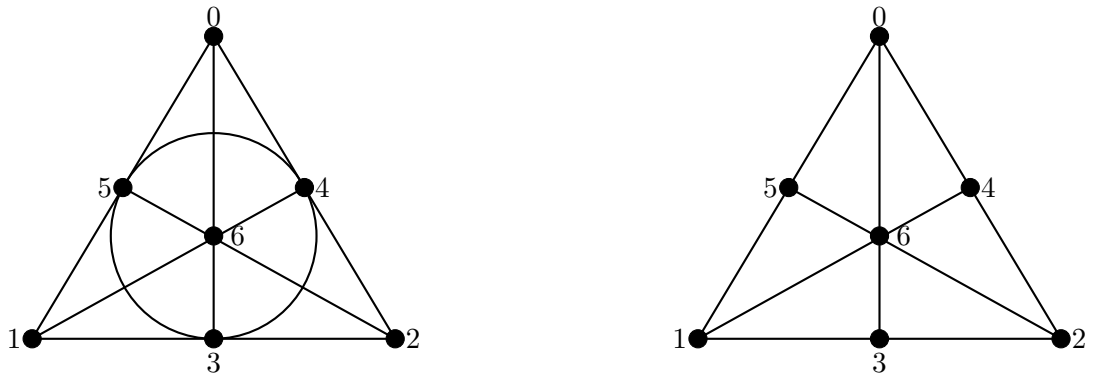
For a polymatroid $\mathcal{S} = (Q, r)$ and a set $B \subseteq Q$, the *deletion* $\mathcal{S} \setminus B$ *of* B *from* $\mathcal{S}$ is the polymatroid $(Q \setminus B, \widehat{r})$ with $\widehat{r}(X) = r(X)$ for every $X \subseteq Q \setminus B$, while the *contraction* $\mathcal{S}/B = (Q \setminus B, \widetilde{r})$ *of* B *from* $\mathcal{S}$ is defined by $\widetilde{r}(X) = r(XB) - r(B)$ for every $X \subseteq Q \setminus B$. Every polymatroid that is obtained from $\mathcal{S}$ by applying deletions and contractions is called a *minor of* $\mathcal{S}$. Observe that the minors of matroids are also matroids.

Two matroids $\mathcal{M}_1 = (Q_1, \mathcal{I}_1)$ and $\mathcal{M}_2 = (Q_2, \mathcal{I}_2)$ are said to be *isomorphic* if there exists a bijection

$$\psi : Q_1 \to Q_2$$

such that, for every set $X_1 \in Q_1$,

$$X_1 \in \mathcal{I}_1 \iff \psi(X_1) \in \mathcal{I}_2.$$



(A) Fano Matroid (B) Non-Fano Matroid

FIGURE 2.2: Two Linearly Representable Matroids

2.3.1 Matroid Representation

A matroid's linear representation refers to a matrix with elements from a finite field such that columns of this matrix are indexed by elements of the matroid's ground set, and subsets are dependent/independent if and only if their corresponding columns are linearly dependent/independent. Not all matroids have a matrix that satisfies this condition. Algebraic representation on the other hand has to do with algebraic field extensions. Formal definitions are given below.

Definition 2.15. A matroid $\mathcal{M} = (Q, r)$ is *ℓ-linearly representable* over a field $\mathbb{F}$ for some $\ell \in \mathbb{N}$ if there exists a vector space $\mathcal{V}$ and a vector subspace collection $(V_x)_{x \in Q}$ defined over $\mathbb{F}$ with $V_x \subseteq \mathcal{V}$ such that

$$\dim\left(\sum_{x \in A} V_x\right) = \ell \cdot r(A) \text{ for every } A \subseteq Q.$$

If the matroid is 1-linearly representable over any field $\mathbb{F}$ we simply say the matroid is a *(linearly) representable* matroid. Otherwise, we call it a *non-representable* matroid. Observe that matroids that are ℓ-linearly representable for some $\ell > 1$ are called *folded-linear* matroids in this thesis. Such matroids are called *multilinear* matroids in the literature, but because there is no multilinear algebra involved, we use a different term instead. Our term comes from the analogy with folded Reed-Solomon codes.

An example of a linearly representable matroid is the following. Consider the following matrix that takes values over a field $\mathbb{F}$ of characteristic 2.

$$\begin{array}{c} \begin{matrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} \end{array} \tag{2.9}$$

A matroid on this matrix consists of the ground set $Q = \{0, 1, 2, 3, 4, 5, 6\}$ where a subset $A \subseteq Q$ is independent if and only if the submatrix indexed by the elements of A is linearly independent over $\mathbb{F}$. This is in fact the *Fano* matroid shown in Fig. 2.2a.

If, however, the field $\mathbb{F}$ is of characteristic other than 2, then this matrix represents the *non-Fano* matroid in Fig. 2.2b.

Consider a field $\mathbb{F}$ and another field $\mathbb{K}$ such that $\mathbb{F} \subseteq \mathbb{K}$ and operations on $\mathbb{F}$ are restrictions of same operations on $\mathbb{K}$. Then $\mathbb{K}$ is called an *extension* of $\mathbb{F}$. An element x of $\mathbb{K}$ is said to be *algebraic* over $\mathbb{F}$ if it is the root of some non-trivial polynomial in $\mathbb{F}$. Otherwise it is *transcendental*. If every element x of $\mathbb{K}$ is algebraic over $\mathbb{F}$, then $\mathbb{K}$ is called an *algebraic extension* of $\mathbb{F}$. Given a subset $X \subseteq \mathbb{K}$, an element y of $\mathbb{K}$ is *algebraically independent* with respect to X if it is transcendental over the field $\mathbb{F}(X)$. A subset $X \subseteq \mathbb{K}$ is *algebraically independent* over $\mathbb{F}$ if every element $x \in X$ is algebraically independent with respect to the set $X \setminus x$ (i.e., no element $x \in X$ is the root of some non-trivial polynomial in $\mathbb{F}(X \setminus x)$), and *algebraically dependent* otherwise. The *transcendence degree* of $\mathbb{K}$ over $\mathbb{F}$ is the size of the largest algebraically independent subset of $\mathbb{K}$ over $\mathbb{F}$.

Definition 2.16. A matroid $\mathcal{M} = (Q, r)$ is *algebraically representable* over a field $\mathbb{F}$ if there exist an extension $\mathbb{K}$ of $\mathbb{F}$ and a sequence of elements $(e_i)_{i \in Q} \subseteq \mathbb{K}$ such that, for every $A \subseteq Q$,

$$r(A) = \deg_{tr} \mathbb{F}((e_i)_{i \in A}),$$

where $\mathbb{F}((e_i)_{i \in A})$ is the smallest field containing $(e_i)_{i \in A}$ and $\deg_{tr}$ is the transcendence degree of $\mathbb{F}((e_i)_{i \in A})$ over $\mathbb{F}$.

Fujishige [55] observed that, given a set $P = \{1, \ldots, n\}$ with an associated set of random variables $\{S_1, \ldots, S_n\}$, the entropy function $h : 2^P \to \mathbb{R}_{\geq 0}$ on this set expressed as

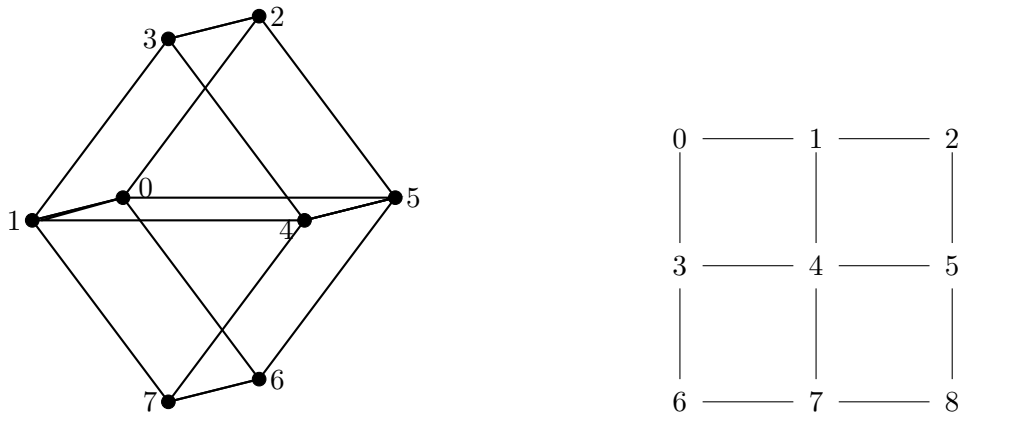
$$h(A) = H(S_A)$$

for every $A \subseteq P$ such that $A \neq \emptyset$ and $h(\emptyset) = 0$, defines the rank function of a polymatroid. That is, P is the ground set of the polymatroid (P, h). In the literature, (P, h) is called an *entropic polymatroid*. A matroid is said to be *almost entropic* if it is the limit of a sequence of entropic polymatroids, and *entropic* if its rank function is a multiple of the rank function of an entropic polymatroid.

Some matroids are more commonly known than others. Two prominent matroids that we will see a lot of in this thesis are the *Vámos* and the *Tic-Tac-Toe* matroids.

The Vámos matroid (Fig. 2.3a) is a sparse-paving, self-dual rank-4 matroid on 8 points named after the English mathematician who first described it, Peter Vámos. Its circuit-hyperplanes are the sets $\{0, 1, 2, 3\}$, $\{0, 1, 4, 5\}$, $\{0, 1, 6, 7\}$, $\{2, 3, 4, 5\}$ and $\{4, 5, 6, 7\}$. It is a special matroid, being one of the smallest non-representable matroids over any field. Its non representability stems from the fact that the set $\{2, 3, 6, 7\}$ is not a circuit-hyperplane. It is also one of the smallest non-algebraic matroids.

The Tic-Tac-Toe matroid is a sparse-paving Ingleton-compliant rank-5 matroid on 9 points. Its name comes from the fact that the relationship between its 8 circuit-hyperplanes can be pictorially represented using the diagram of the Tic-Tac-Toe game (see Fig. 2.3b). Its circuit-hyperplanes are the sets $\{0, 1, 2, 3, 6\}$, $\{0, 1, 2, 4, 7\}$, $\{0, 1, 2, 5, 8\}$, $\{0, 3, 4, 5, 6\}$, $\{2, 3, 4, 5, 8\}$, $\{0, 3, 6, 7, 8\}$, $\{1, 4, 6, 7, 8\}$ and $\{2, 5, 6, 7, 8\}$. The Tic-Tac-Toe matroid is non-representable over any field. Neither is its dual. While its dual has been proven to be non-algebraic [60], the algebraicity of Tic-Tac-Toe is an open question. Tic-Tac-Toe is widely regarded as a prime example of a specimen to solve the question of whether or not algebraicity is preserved by duality.



(A) Vámos Matroid (B) Tic-Tac-Toe Matroid

FIGURE 2.3: Some Non-linearly Representable Matroids

2.3.2 Matroid Intersection Properties

In this section, we introduce 3 intersection properties that were shown to be satisfied by linearly representable matroids.

We begin with two important definitions.

Definition 2.17. Given a matroid $\mathcal{M} = (Q, r)$, a *modular cut* $\mathcal{F}$ of $\mathcal{M}$ is a family of flats of $\mathcal{M}$ satisfying the following properties:

1. For every $F_1 \in \mathcal{F}$ and for every flat F_2 such that $F_1 \subseteq F_2$, $F_2 \in \mathcal{F}$, i.e., $\mathcal{F}$ is monotone increasing.
2. For every modular pair $F_1, F_2 \in \mathcal{F}$, $F_1 \cap F_2 \in \mathcal{F}$, i.e., $\mathcal{F}$ is closed under intersection of modular pairs.

Definition 2.18. Given a matroid $\mathcal{M} = (Q, r)$, a *proper point extension* of $\mathcal{M}$ by a point p is an extension in which the corresponding modular cut is a proper subset of the lattice of flats of $\mathcal{M}$.

Every proper point extension of a matroid corresponds to a modular cut and vice versa [91, Section 7.2]. The modular cut *generated* by the flats $\{F_1, F_2, \ldots, F_k\}$, for some $k > 0$ is simply the smallest modular cut that contains these flats.

Bachem and Wanka [9] introduced three intersection properties satisfied by all linearly representable matroids.

Definition 2.19 (EP)**.** A matroid $\mathcal{M}$ is said to satisfy the *Euclidean intersection property* if for every non-intersecting pair of hyperplane H and line ℓ of $\mathcal{M}$, there is a proper point extension $\mathcal{M}'$ of $\mathcal{M}$ by an element p such that p lies in the intersection of the $\mathcal{M}'$ closures of H and ℓ.

Definition 2.20 (GP)**.** A matroid $\mathcal{M}$ is said to satisfy the *generalized Euclidean intersection property* if for every non-modular pair of flats X and Y of $\mathcal{M}$, there is a proper point extension $\mathcal{M}'$ of $\mathcal{M}$ by an element p such that p lies in the intersection of the $\mathcal{M}'$ closures of X and Y.

Definition 2.21 (LP)**.** A matroid $\mathcal{M}$ of rank d is said to satisfy *Levi's intersection property* if for every $d-1$-tuple of hyperplanes $(H_i)_{i\in[d-1]}$ of $\mathcal{M}$ such that $\cap_{i=1}^{d-1} H_i = \emptyset$, there is a proper point extension $\mathcal{M}'$ of $\mathcal{M}$ by an element p such that p lies in the intersection of the $\mathcal{M}'$ closures of $(H_i)_{i\in[d-1]}$.

Let $\mathcal{M}_{LP}, \mathcal{M}_{GP}, \mathcal{M}_{EP}$ represent the class of matroids that satisfy the LP, GP, and EP properties, respectively, and let $\mathcal{M}_{lin}$ be the class of linear matroids. Bachem and Wanka [9] proved the following results with respect to these classes. In the first one, they show that there is an inclusion relationship between these matroids and the class of linear matroids. They then go on to show that these 3 classes are equivalent for rank-4 matroids.

Proposition 2.22. *[9, Prop. 2]* $\mathcal{M}_{lin} \subseteq \mathcal{M}_{LP} \subseteq \mathcal{M}_{GP} \subseteq \mathcal{M}_{EP}$.

Proposition 2.23. *[9, Cor. 4] Let* $\mathcal{M}^4_{LP}, \mathcal{M}^4_{GP}, \mathcal{M}^4_{EP}$ *represent the class of rank-4 matroids that satisfy the LP, GP, and EP properties, respectively, and let* $\mathcal{M}^4_{lin}$ *be the class of all linearly representable rank-4 matroids. Then*

$$\mathcal{M}^4_{lin} \subseteq \mathcal{M}^4_{LP} = \mathcal{M}^4_{GP} = \mathcal{M}^4_{EP}.$$

All matroids of rank less than 3 are linear and therefore satisfy these intersection properties. In the case of rank-3 matroids, while not all of them are linear, with the non-Pappus and non-Desargues matroids being prime examples, they all satisfy the 3 intersection properties. So the first examples of matroids not satisfying these properties will be matroids of rank 4. The following property is useful when talking about rank-4 matroids. It was introduced in [40].

Definition 2.24. A matroid (Q, r) satisfies the *bundle condition* if it does not contain four flats $(A_i)_{i\in[4]}$ such that every flat has rank 2, the union of every pair of flats has rank 3 except for $r(A_1A_4) = 4$, and the union of every three or four flats has rank 4.

Bachem and Kern [8] showed that the bundle condition is a property of rank-4 matroids that satisfy Levi's intersection property (a simpler sketch of the proof is given in [9]).

Theorem 2.25. *[8, Thm. 9] A rank-4 matroid satisfies the bundle condition if and only if it satisfies Levi's intersection property.*

2.4 Secret Sharing

We introduce here the cryptographic primitive called secret sharing. While we will present a particular definition, we note that there are other equivalent definitions for the term. A very useful resource for this primitive is the survey conducted by Amos Beimel [13]. The definition we employ is more appropriate when using information theory techniques and in the search for lower bounds on the information ratio using information inequalities. We will see more of this later.

Definition 2.26. Let P be a finite set of size n called the set of participants. An *access structure* Γ on P is a monotone increasing family of subsets of P (i.e., for every $A \subseteq P$, if $A \in \Gamma$, then every superset of A is also in Γ).

Due to its monotonicity it is easy to see that Γ can be fully characterized by its family of *minimal* sets, that is, every set A such that $A \setminus a \notin \Gamma$ for every $a \in A$. We denote this minimal family as $\min \Gamma$. An access structure is *connected* if every participant is in at least one minimal set. Similar to matroids and polymatroids we can also define the dual of an access structure. This is the access structure Γ^* given by

$$\Gamma^* := \{A \subseteq P : P \setminus A \notin \Gamma\}.$$

Security definitions of cryptographic schemes can be either unconditional or computational. We say that a cryptographic scheme or protocol is *unconditionally secure* if it is secure regardless of how much computing power is available to an adversary, and it is said to be *computationally secure* if its security is dependent on the adversary's computing power. Below we give an unconditionally secure definition of secret sharing schemes.

Definition 2.27. Let P be as defined above and let $Q = P \cup p_0$. A *secret sharing scheme* on P is a random vector $\Sigma = (S_x)_{x \in Q}$ such that

1. $H(S_{p_0}) > 0$.
2. $H(S_{p_0}|S_P) = 0$.

The special participant p_0 is called the *dealer*. The random variable S_{p_0} corresponds to the *secret value*, and the *share* for a player $x \in P$ is given by the random variable S_x. A set A is *authorized* if $H(S_{p_0}|S_A) = 0$, and *forbidden* if $H(S_{p_0}|S_A) = H(S_{p_0})$. A secret sharing scheme Σ is said to *realize* an access structure Γ if Γ is the family of authorized sets of Σ. Alternatively, we say Γ *admits* Σ. Note that it is sometimes possible for a forbidden subset of participants to still get some information about the secret. Any secret sharing scheme in which forbidden subsets of participants get no information whatsoever about the secret is called a *perfect secret sharing scheme*. All secret sharing schemes in this thesis are assumed to be perfect.

2.4.1 Threshold Secret Sharing

Some secret sharing schemes are such that the determining factor of whether a set is authorized or not is its size. Such secret sharing schemes are known as *threshold secret sharing schemes*. More formally, given a parameter $t \leq n$, a (t, n)-threshold secret sharing scheme Σ is a secret sharing scheme in which all sets A such that $|A| \geq t$ are authorized and other sets are forbidden. Threshold secret sharing schemes were introduced by Shamir [102] and Blakley [26] independently in 1979 as the first types of secret sharing schemes. The Shamir and Blakley schemes were also the first linear secret sharing schemes introduced, as they are defined over finite fields. They are also perfect and ideal since the shares and secret are from the same field, and sets with size less than t learn nothing about the secret.

We illustrate the mechanism of the Shamir secret sharing scheme below.

Example 2.1. *Let s be the secret to be shared and let $[n]$ be the set of participants in the (t, n)-threshold scheme for some $t \leq n$. Take a prime number q such that $q \geq \max\{n, s\}$ and let $\mathbb{F}_q$ be a finite field. Let f_0 be the field element representing the secret and let*

$f_1, \ldots, f_{t-1}$ be random field elements. Also, let $(a_i)_{1\leq i\leq n}$ be distinct field elements called identifiers *assigned to each participant. Then the evaluation of the polynomial*

$$f(x) = f_0 + f_1 x + f_2 x^2 + \ldots + f_{t-1}x^{t-1}$$

at the points $a_1, \ldots, a_n$ is a sharing of the secret f_0. Observe that this sharing can in fact be represented using matrix form and operation as:

$$\begin{pmatrix} s & s_1 & \cdots & s_n \end{pmatrix} = \begin{pmatrix} f_0 & f_1 & \cdots & f_{t-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & a_1 & a_2 & \cdots & a_n \\ 0 & a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & a_1^{t-1} & a_2^{t-1} & \cdots & a_n^{t-1} \end{pmatrix}. \tag{2.10}$$

Now for members of a set $A \subseteq [n]$ to reconstruct the secret f_0, members need to, in principle, reconstruct the polynomial f and then evaluate it at 0, since $f(0) = f_0 = s$. The idea behind this is to use Lagrange polynomial interpolation to reconstruct f. To do this, however, we must have that $|A| \geq t$ since it requires at least t evaluation points to reconstruct a polynomial of degree $t-1$. The Lagrange polynomial in this case is given as

$$f(x) = \sum_{i\in A} s_i \prod_{j\in A, j\neq i} \frac{x - a_j}{a_i - a_j}.$$

Observe that the choice of all a_i being distinct ensures that $a_i - a_j \neq 0$ in the fraction above. Hence, to recover the secret, members of A with $|A| \geq t$ only need to compute

$$s = \sum_{i\in A} s_i \prod_{j\in A, j\neq i} \frac{a_j}{a_j - a_i}$$

over the field $\mathbb{F}_q$.

2.4.2 Linear Secret Sharing Schemes

The following definition of linear secret sharing schemes appears in [92, **Sec. 1.6**].

Definition 2.28. Let $\mathbb{F}$ be a finite field and let $(E_i)_{i\in Q}$ be a family of vector spaces over $\mathbb{F}$. Let $\pi : E \to E_i$ be an injective map over $\mathbb{F}$ such that each of the induced maps $\pi_i : E \to E_i$ is surjective. Suppose we take the uniform probability distribution on E. Then each map π_i defines a random variable S_i on E_i for every $i \in Q$, and $(S_i)_{i\in Q}$ is called a $\mathbb{F}$-*linear* family of random variables.

A secret sharing scheme $\Sigma = (S_x)_{x\in Q}$ is called a $\mathbb{F}$-*linear secret sharing scheme* if $(S_x)_{x\in Q}$ is a $\mathbb{F}$-*linear* family of random variables.

If $\dim(E_0) = \ell$, then we call Σ an $(\mathbb{F}, \ell)$-linear secret sharing scheme or simply an ℓ-linear secret sharing scheme if the field is not important.

Linear secret sharing schemes have the property that all the mappings π_i can be represented using a matrix with elements from the field $\mathbb{F}$. The convention is to use each column to represent the participants of the scheme with the first column being assigned to the dealer, but in some cases more than one column is assigned to a participant. Each row represents a sharing of the secret in the first entry of that row. Hence, no two rows are the same. In fact, the secret sharing scheme given in Example 2.1 is a linear scheme.

2.4.3 Efficiency Measures of Secret Sharing Schemes

There are a number of ways to measure how efficient a secret sharing scheme is, with each one looking at different aspects of a secret sharing scheme. The first one we will mention is the *share size* of the scheme. By this, we mean the maximum of the size of the shares in bits given to each participant. This is the most fundamental and natural efficiency measure of a secret sharing scheme as it looks at how much information in bits each participant needs to have for the scheme to be correct. There's also the *total share size* which sums the size of all the shares in the scheme. Another efficiency measure is the complexity of the sharing and reconstruction protocols of the scheme. This looks at the steps involved in sharing the secret and also in using shares from authorized sets to recover the secret.

A third kind of efficiency measure is the information ratio. This is a measure that relates the size of the shares of each participant in the scheme to the size of the secret. This is the efficiency measure we consider in this thesis as it is more adapted to information-theoretic measures. We give a formal definition below.

Definition 2.29. Let $\Sigma = (S_x)_{x\in Q}$ be a secret sharing scheme. The *information ratio* of the secret sharing scheme Σ is given as

$$\sigma(\Sigma) = \max_{x\in P} \frac{H(S_x)}{H(S_{p_0})}.$$

Also, its *average information ratio* is given as

$$\widetilde{\sigma}(\Sigma) = \frac{1}{n}\sum_{x\in P} \frac{H(S_x)}{H(S_{p_0})}.$$

The *total* information ratio is given as $n \cdot \widetilde{\sigma}(\Sigma)$.

The information ratio, however, is not without its own drawback. Some schemes have constant size information ratios but have the disadvantage that the secret and shares are doubly exponential. In cases like these, while the scheme might be deemed efficient because of the constant information ratio, the share size makes it impractical to use. On the other hand, the information ratio is sometimes easier to work with since there are already a number of established ways to find bounds on it.

Karnin et al. [69] established that the size of the shares of each participant in a perfect secret sharing scheme Σ must be at least the size of the secret. When the size of the shares is exactly the size of the secret, Σ is called an *ideal* secret sharing scheme. Access structures that admit ideal schemes are called *ideal* access structures.

For an access structure Γ, its *optimal information ratio*, denoted $\sigma(\Gamma)$ is the infimum of the information ratios of all secret sharing schemes that realize Γ and is written as

$$\sigma(\Gamma) = \inf\{\sigma(\Sigma) : \Sigma \text{ is a secret sharing scheme that realizes } \Gamma\}.$$

The *optimal average information ratio* $\widetilde{\sigma}(\Gamma)$ of Γ is the infimum of the average information ratios of all secret sharing schemes that realize Γ and is written

$$\widetilde{\sigma}(\Gamma) = \inf\{\widetilde{\sigma}(\Sigma) : \Sigma \text{ is a secret sharing scheme that realizes } \Gamma\}.$$

If, instead, we only consider linear secret sharing schemes that realize Γ, then we denote the optimal information ratio as $\lambda(\Gamma)$ and the optimal average information ratio as $\widetilde{\lambda}(\Gamma)$. An *optimal secret sharing scheme* Σ is such that $\sigma(\Sigma) = \sigma(\Gamma)$.

Csirmaz [36] found that the best lower bound on the information ratio in a secret sharing scheme on n participants is $\Omega(n/\log n)$. Using a general construction, the first upper bound on the information ratio of schemes with a 1-bit secret was shown to be $2^{O(n)}$. Specific bounds have been obtained since. Liu and Vaikuntanathan [75] obtained a $2^{0.994n}$ bound on the share size for general access structures and $2^{0.999n}$ for linear schemes. Applebaum et al. [5] reduced these to $2^{0.892n}$ and $2^{0.942n}$, respectively. Also, Applebaum et al. [6] improved these to $2^{0.637n}$ and $2^{0.762n}$, respectively.

2.4.4 Secret Sharing and Polymatroids

Let (P, h) be an entropic polymatroid. Recall that for every $A \subseteq P$, $h(A) = H(S_A)$ where S_A is a random variable associated to A. Now suppose we define a function $f : 2^P \to \mathbb{R}_+$ as

$$f(X) = \frac{h(X)}{H(S_{p_0})}$$

where p_0 is a special element with an associated random variable S_{p_0} such that $H(S_{p_0}) > 0$ and, for every $X \subseteq P$ we have that either $f(Xp_0) = f(X)$ or $f(Xp_0) = f(X) + 1$. Then, for $Q = Pp_0$, the set

$$\Gamma_{p_0} = \{X \subseteq P : f(Xp_0) = f(X)\}$$

is in fact the access structure of a secret sharing scheme, the special element p_0 is the dealer and S_{p_0} is the random variable associated to the secret, and the random variables $(S_x)_{x \in Q \setminus p_0}$ are the random variables associated to the shares of the participants of the scheme. Whenever $\mathcal{M}_{p_0} = (Q, f)$ is a matroid, the access structure Γ_{p_0} is called the *port of the matroid at* p_0 or just simply a *matroid port*. Matroid ports were introduced by Lehman [71] in 1964 but in a different context and with a different definition.

Brickell and Davenport [31] observed that every connected ideal secret sharing scheme defines a matroid. As a result of this, we see that every ideal access structure is in fact a matroid port. The reverse of this, however, is not true. This was proved by Seymour [101] in 1992 when he showed that the Vamos matroid is not a "secret-sharing" matroid.

We recall the definition of circuits of a matroid as all minimal sets X such that $r(X \setminus p) < r(X)$ for all $p \in X$. Evidently then, the minimal access structure of Γ_{p_0} whenever Γ_{p_0} is a matroid port is therefore the set of all circuits of $\mathcal{M}$ containing p_0. That is,

$$\min \Gamma_{p_0} = \{C \subseteq P : C \cup \{p_0\} \text{ is a circuit}\}.$$

Observe that, for any set $A \subseteq P$ in $\mathcal{M}_{p_0} = (Q, f)$, we have

$$f(p_0|A) = f(A \cup p_0) - f(A) \leq f(p_0) = 1.$$

Now, since $\mathcal{M}_{p_0}$ is a matroid, we know that its rank function is integer valued, hence for all $A \subseteq P$, we have that

$$f(p_0|A) \in \{0, 1\}.$$

An immediate consequence of this is that the matroid port Γ_{p_0} is a perfect access structure.

We saw in Section 2.3 that a matroid is uniquely determined by its circuits. Lehman went further to show that every connected matroid is uniquely determined by the set of circuits containing some particular point. This idea comes in handy here to show that every matroid port is unique to its matroid. Hence, if Γ is a connected matroid port, then there exists a unique connected matroid $\mathcal{M}$ for which $\Gamma = \Gamma_{p_0}(\mathcal{M})$.

Chapter 3

Common Information and Matroid Representation

3.1 Introduction

In this chapter, we introduce the two main tools central to our work: the *common information* and *AK-information* properties. Many non-Shannon-type rank inequalities are derived using the common information property while the AK information is used to derive non-Shannon-type information inequalities. Inequalities derived using these properties are then applied to the search for lower bounds in secret sharing. In this chapter, however, we show how to apply these properties to the problem of matroid representation.

First, we discuss these information properties in Section 3.3. Then in Section 3.4, we give the linear programming problems derived from using these properties for the purpose of studying matroid classification problems.

In Section 3.5, we discuss CI-compliant polymatroids. We show that the CI property is preserved by the taking of minors. Hence, minors of CI-compliant matroids are also CI-compliant. This will be useful when studying larger matroids. Instead of directly checking if the matroid is CI-compliant, an option would be to find if it contains a non-CI-compliant matroid, much like using excluded minors to find non-representable matroids.

In the penultimate section of this chapter, we discuss some other linear programming problems that might be useful in the classification of matroids. Our focus is placed on generalizations of the Ingleton-Main Lemma (a tool useful for detecting non-algebraic matroids).

The final section contains discussion on the optimizations of the LP technique using CI and AK, and also an optimization result of the Zhang-Yeung inequality. First, we show that it is enough to take non-modular pairs of flats for CI. And then applying some other results, we prove that for AK it is enough to take (U, V, Z) such that UV and Z are a non-modular pair.

Much like the Ingleton inequality is satisfied by linearly representable matroids, the Zhang-Yeung inequality is satisfied by almost entropic matroids [83]. And in the spirit

of [57] for the Ingleton inequality, we give some optimizations that might help reduce the computation time of checking that a matroid satisfies the Zhang-Yeung inequality.

3.1.1 Common Information

Besides Ingleton and Zhang–Yeung inequalities, many other linear information and rank inequalities have been found [41, 43, 44, 70, 77, 81]. Nevertheless, only a few techniques to derive such inequalities are known, and it appears that many more inequalities remain unknown.

Linear information and rank inequalities are fundamental in the linear programming technique that has been used to find bounds on the information ratio of secret sharing schemes [18, 19, 79, 89, 93] and on the achievable rates in network coding [42, 106, 111]. An improvement to that technique has been recently proposed [50]. Specifically, instead of known inequalities, the properties from which most linear information and rank inequalities are derived are used as constraints. The notion of *common information* of two random variables is at the core of most of those properties. Most of the known linear information inequalities are obtained from the concept of *AK-common information*, derived from Ahlswede–Körner lemma [1, 2, 39], or from the *copy lemma* [41, 44]. According to [43], all linear rank inequalities that were known in 2009 were derived from the *common information property* and, to the best of our knowledge, that is still the case nowadays. Nevertheless, some restricted linear rank inequalities have been presented since then. Namely, *characteristic-dependent* inequalities [45, 94], which are satisfied by all polymatroids that are linearly representable over fields of a given characteristic.

3.1.2 Matroid Representation

Relevant applications in information theory, especially in secret sharing and network coding, brought to light the class of *entropic* matroids, which contains the well-known class of linear matroids.

An *entropic vector* is formed by the joint Shannon entropies of all subsets of a finite set of discrete random variables. Every entropic vector is the rank function of a polymatroid. A polymatroid is *entropic* if its rank function is a multiple of an entropic vector. Limits of entropic polymatroids are called *almost entropic*. Both representation by partitions [80] and by almost affine codes [104] are characterizations of entropic matroids.

In the same way that linear matroids are defined from configurations of vectors in a vector space, configurations of vector subspaces determine *linear polymatroids*. A *folded linear* matroid is such that some multiple of its rank function corresponds to a linear polymatroid. Folded linear matroids have been called *multilinear* or *multilinearly representable* in the literature. Since no multilinear algebra is involved, that terminology may be misleading. The name proposed here is motivated by the analogy with folded Reed-Solomon codes.

It is well known that linear polymatroids and, consequently, folded linear matroids are entropic. František Matúš [82] recently proved that algebraic matroids are almost entropic.

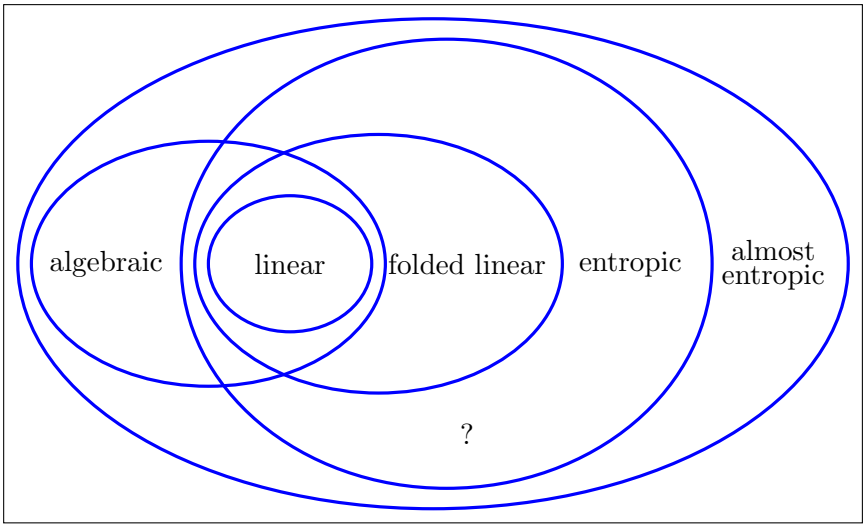


FIGURE 3.1: A classification of matroids. Discussed in Section 3.2.

Figure 3.1, an update of the corresponding diagram in [83], illustrates the current knowledge about the connections between the aforementioned classes of matroids. A detailed explanation is given in Section 3.2. There is a number of tools to deal with that classification. Among them, linear information and rank inequalities are especially useful. *Linear information inequalities*, such as Zhang–Yeung inequality [114], are the linear inequalities that are satisfied by the rank function of every entropic polymatroid. The ones that, like Ingleton inequality [61], are satisfied by the rank function of every linear polymatroid are called *linear rank inequalities*.

Ingleton inequality was used to prove the existence of an infinite number of excluded minors for the class of matroids that are linear over any given infinite field [86]. That result has been extended to the class of folded linear matroids over any given field and, by using Zhang–Yeung inequality instead of Ingleton inequality, to the classes of almost entropic matroids and algebraic matroids [83].

3.2 Polymatroid Representations

For a positive integer m, we notate $[m] = \{1, \ldots, m\}$. We use a compact notation for set unions, that is, we write XY for $X \cup Y$ and Xy for $X \cup \{y\}$. In addition, we write $X \smallsetminus Y$ for the set difference and $X \smallsetminus x$ for $X \smallsetminus \{x\}$. The reader should be aware that this is slightly different operation symbol from that used in polymatroid deletions, for example.

Let $S = (S_x)_{x \in Q}$ be a discrete random vector, that is, a finite sequence of discrete random variables. For every $X \subseteq Q$, take $h(X) = H(S_X)$, the Shannon entropy of the discrete random variable $S_X = (S_x)_{x \in X}$. Then $(h(X))_{X \in \mathcal{P}(Q)}$ is the *entropic vector* associated to S. Because of the basic properties of Shannon entropy, every entropic vector is the rank function of a polymatroid [54, 55]. A polymatroid is *entropic* if its rank function is a multiple of an entropic vector. The closure in $\mathbb{R}^{\mathcal{P}(Q)}$ of the set of entropic vectors is a convex cone [111]. Each element in this convex cone is the rank function of an *almost entropic* polymatroid.

We introduce next some notation that is motivated by this connection between Shannon entropy and polymatroids. By analogy with the conditional mutual information, for a polymatroid (Q, f) and sets $X, Y, Z \subseteq Q$, we write

$$f(Y{:}Z|X) = f(XY) + f(XZ) - f(XYZ) - f(X)$$

and, in particular, $f(Y{:}Z) = f(Y{:}Z|\emptyset) = f(Y) + f(Z) - f(YZ)$ and $f(Y|X) = f(Y{:}Y|X) = f(XY) - f(X)$.

Consider a field $\mathbb{F}$, a vector space V with finite dimension over $\mathbb{F}$ and a collection $(V_x)_{x\in Q}$ of vector subspaces of V. It is clear from basic linear algebra that the map f defined by $f(X) = \dim \sum_{x\in X} V_x$ for every $X \subseteq Q$ is the rank function of a polymatroid. Every such polymatroid is said to be *linearly representable*, or simply *linear*, over $\mathbb{F}$. For a positive integer k, a *k-folded $\mathbb{F}$-linear* matroid (Q, r) is such that the polymatroid (Q, kr) is $\mathbb{F}$-linear. As we mentioned in the Introduction, folded linear matroids are also called *multilinear* or *multilinearly representable* in the literature.

Suppose now that $\mathbb{F}$ is a finite field and take the dual vector space V^*. The uniform probability distribution on V^* and the projections $V^* \to V_x^*$ for $x \in Q$ determine a discrete random vector $(S_x)_{x\in Q}$. Such random vectors are called *linear*. The entropic vector h associated to S satisfies $h(X) = f(X) \log |\mathbb{F}|$ for every $X \subseteq Q$. Since every linear polymatroid admits a linear representation over some finite field [98], linear polymatroids and folded linear matroids are entropic.

Given a positive integer m, a collection $(A_i)_{i\in[m]}$ of subsets of a finite set Q, and $I \subseteq [m]$, we notate $A_I = \bigcup_{i\in I} A_i$. A *linear information inequality*, respectively *linear rank inequality*, on m variables consists of a collection $(\alpha_I)_{I\in\mathcal{P}([m])}$ of real numbers such that $\sum_{I\in\mathcal{P}([m])} \alpha_I f(A_I) \geq 0$ for every entropic, respectively linear, polymatroid (Q, f) and for every collection $(A_i)_{i\in[m]}$ of subsets of Q. Since every linear polymatroid is entropic, every information inequality is also a rank inequality.

Folded linear matroids are entropic. Every linear matroid is algebraic [91]. It has been recently proved that every algebraic matroid is almost entropic [82]. Vámos matroid is not almost entropic because it does not satisfy Zhang–Yeung inequality. Non-Pappus matroid is a folded linear matroid that is algebraic but not linear [91, 104]. Two examples of almost entropic matroids that are not entropic were given in [83, Remarks 4, 5]. Only one of them is algebraic. A folded linear matroid that is not algebraic was presented in [22]. It is not known if there exist entropic matroids that are not folded linear. These facts are illustrated in Figure 3.1.

For every positive integer k and any field $\mathbb{F}$, the class of k-folded $\mathbb{F}$-linear matroids is closed by duality [64, 91]. It is unknown whether or not this is the case for the classes of algebraic or entropic matroids. Remarkably, Kaced [67] recently proved that the class of almost entropic matroids is not closed by duality. An explicit counterexample is presented in [37].

Every minor of an $\mathbb{F}$-linear polymatroid is $\mathbb{F}$-linear. That is, the class of $\mathbb{F}$-linear polymatroids is closed under minors. The same applies to the class of almost entropic polymatroids [84, Lemma 1]. The classes of linear, folded linear, algebraic [91, Corollary 6.7.14], and almost entropic matroids are closed under minors.

3.3 How to Use Undiscovered Information and Rank Inequalities

The title of this section is borrowed from [58]. It precisely describes the main idea behind the technique introduced in [50], namely, using properties from which information and rank inequalities have been derived instead of using known inequalities.

3.3.1 Common Information

We say that a random variable S_3 *conveys the common information* of the random variables S_1 and S_2 if $H(S_3|S_2) = H(S_3|S_1) = 0$ and $H(S_3) = I(S_1{:}S_2)$. In general, given two random variables, it is not possible to find a third one satisfying those conditions [56]. Nevertheless, this is possible for every pair of random variables in a linear random vector. Most of the known non-Shannon rank inequalities are derived from this fact [43]. A combinatorial abstraction of the notion of common information is given in the next definition.

Definition 3.1. Let (Q, f) be a polymatroid and let $A, B \subseteq Q$. Then every subset $X_o \subseteq Q$ satisfying

(C1) $f(X_o|A) = f(X_o|B) = 0$, and

(C2) $f(X_o) = f(A{:}B)$

is called a *common information for the pair* (A, B). If $X_o = \{x_o\}$, then the element x_o is also called a common information for the pair (A, B).

Definition 3.2. Consider polymatroids (Q, f) and (Q', f') with $Q \subseteq Q'$. We say that (Q', f') is an *extension* of (Q, f) if $f(X) = f'(X)$ for every $X \subseteq Q$. In this situation we will generally use the same symbol for both rank functions.

Definition 3.3. A polymatroid (Q, f) is *1-CI-compliant* if, for every pair (A, B) of subsets of Q, there exists an extension (Qx_o, f) such that x_o is a common information for the pair (A, B). Inductively, for every integer $k > 1$, a polymatroid $\mathcal{S} = (Q, f)$ is *k-CI-compliant* if, for every pair (A, B) of subsets of Q, there exists an extension (Qx_o, f) such that x_o is a common information for the pair (A, B) and (Qx_o, f) is $(k-1)$-CI-compliant. A polymatroid is *CI-complaint* if it is k-CI-compliant for every positive integer k.

Proposition 3.4. *Let $\mathbb{F}$ be a field. Consider an $\mathbb{F}$-linear polymatroid (Q, f) and a pair (A, B) of subsets of the ground set. Then there exists an $\mathbb{F}$-linear extension (Qx_o, f) such that x_o is a common information for (A, B). As a consequence, linear polymatroids and, in particular, folded linear matroids are CI-compliant.*

Proof. Consider a collection $(V_x)_{x\in Q}$ of vector subspaces providing an $\mathbb{F}$-linear representation of (Q, f). For every $X \subseteq Q$, put $V_X = \sum_{x\in X} V_x$. Given a pair (A, B) of subsets of Q, take $V_{x_o} = V_A \cap V_B$. Then $(V_x)_{x\in Qx_0}$ is an $\mathbb{F}$-linear representation of a polymatroid (Qx_0, f) extending (Q, f) in which x_0 is a common information for (A, B). □

3.3.2 Ahlswede and Körner's Information

Linear information inequalities can be derived from properties that are satisfied by every almost entropic polymatroid. Specifically, all known linear information inequalities have been derived from the copy lemma [114] and the Ahlswede–Körner lemma [1, 2, 39] as used in [77].

Definition 3.5. Let (Q, f) be a polymatroid, and let $U, V, Z \subseteq Q$. Then every subset $Z_o \subseteq Q$ such that

(AK1) $f(Z_o|UV) = 0$,

(AK2) $f(U|Z_o) = f(U|Z)$ and $f(V|Z_o) = f(V|Z)$,

(AK3) $f(UV|Z_o) = f(UV|Z)$

is called an *AK-information for the triple* (U, V, Z).

We say that a polymatroid (Q, f) is *1-AK-compliant* if, for every triple (U, V, Z) of subsets of Q, there exists an extension (Qz_o, f) such that z_o is an AK-information for the triple (U, V, Z). Analogously to the discussion on the common information property, we can define *k-AK-compliance* for every $k > 0$ and also *AK-compliance*. Next proposition was proved in [50] from [77, Lemma 5] and [66, Lemma 2]. As a consequence, almost entropic polymatroids are AK-compliant.

Proposition 3.6. *For every almost entropic polymatroid (Q, f) and sets $U, V, Z \subseteq Q$, there exists an almost entropic extension (Qz_o, f) such that z_o is an AK-information for the triple (U, V, Z).*

As consequence of the following result from [50], k-CI-compliant polymatroids are also k-AK-compliant.

Proposition 3.7. *If x_o is a common information for the pair (UV, Z), then x_o is an AK-information for the triple (U, V, Z).*

3.4 Application of CI and AK to Classification of Matroids

Linear information inequalities provide necessary conditions for a matroid to be almost entropic and, as a consequence of the result in [82], also to be algebraic. The same applies to linear rank inequalities with respect to the class of folded linear matroids. A polymatroid is *Ingleton-compliant*, respectively *ZY-compliant*, if Ingleton inequality (2.8), respectivey Zhang–Yeung inequality (2.7), holds for every collection $(A_i)_{i\in[4]}$ of subsets of the ground set. As a consequence of the proofs for those inequalities [43, 66, 77], 1-CI-compliant and 1-AK compliant polymatroids are Ingleton-compliant and, respectively, ZY-compliant. Those inequalities are related to a special configuration called the *bundle condition* (Def. 2.24) which was introduced in [40].

Vámos matroid is among the smallest ones violating the bundle condition, and the one with the minimum number of dependent hyperplanes. If a matroid does not satisfy

the bundle condition, then the collection $(A_i)_{i\in[4]}$ described in the previous definition violates both Ingleton and Zhang–Yeung inequalities as expressed in (2.8) and (2.7), respectively. Therefore, almost entropic matroids and, in particular, algebraic matroids satisfy the bundle condition. Moreover, the sparse-paving matroids that are Ingleton-compliant coincide with those satisfying a generalization of the bundle condition [90, Corollary 3.2].

Proposition 3.8. *Let $\mathcal{M}$ be a sparse-paving matroid of rank $k \geq 4$. Then $\mathcal{M}$ is not Ingleton-compliant if and only if there exist five pairwise disjoint subsets B, A_1, A_2, A_3, A_4 of the ground set with $|B| = k-4$ and $|A_i| = 2$ such that BA_1A_4 is a basis and all the other sets of the form BA_iA_j with $i \neq j$ are circuit-hyperplanes.*

Corollary 3.9. *If a sparse-paving matroid $\mathcal{M}$ is not Ingleton-compliant, then there is a minor of $\mathcal{M}$ on eight points that is not Ingleton-compliant.*

As a consequence, the class of Ingleton-compliant sparse-paving matroids has a finite number of forbidden minors [90, Theorem 1.3]. In contrast, the set of excluded minors for the class of Ingleton-compliant matroids is infinite [86]. By combining Proposition 3.8 with a recent result about algebraic matroids [82], the following remarkable property of sparse-paving matroids is easily derived.

Theorem 3.10. *If a sparse-paving matroid is not Ingleton-compliant, then it is not ZY-compliant and hence it is neither almost entropic nor algebraic.*

Proof. If a sparse-paving matroid admits the configuration described in Proposition 3.8, then Zhang–Yeung inequality (2.7) does not hold for $(BA_i)_{i\in[4]}$. □

By using the result in Proposition 3.8, Nelson and van der Pol [90] proved that the number of Ingleton-compliant matroids is doubly exponential on the size of the ground set. This indicates that the power of Ingleton inequality in the classification of matroids is quite limited. Of course, many more rank and information inequalities are available, but one may expect a better outcome from the strategy introduced in [50], which makes it possible to use undiscovered inequalities. This claim is supported by the results obtained in secret sharing [50, 58]. Specifically, the linear programming technique discussed in [50] can be adapted to the study of the classes of matroids described in Sections 2.3.1 and 3.2 by using the following linear programming problems or their extensions to multiple pairs or triples of sets.

Linear Programming Problem 1. Given a polymatroid (Q, r), and subsets $A, B \subseteq Q$, determine if there is an extension (Qx_o, r) such that x_o is a common information for the pair (A, B).

Linear Programming Problem 2. Given a polymatroid (Q, r) and subsets $U, V, Z \subseteq Q$, determine if there is an extension (Qz_o, r) such that z_o is an AK-information for the triple (U, V, Z).

Those linear programming problems can be used to disprove that a given matroid is folded linear or almost entropic. Nevertheless, that technique is useless for matroids of rank 3 because they are CI-compliant. The following lemma is a consequence of [91, Proposition 2.1.21].

Lemma 3.11. *Consider a finite set Q and a family $\mathcal{H} \subseteq \mathcal{P}(Q)$ of subsets of Q. Then $\mathcal{H}$ is the family of hyperplanes of a paving matroid of rank 3 on Q if and only if the following properties are satisfied.*

1. *$\mathcal{H}$ has at least two members and every member of $\mathcal{H}$ has at least two elements.*
2. *For every two different elements $x, y \in Q$, there exists a unique $H \in \mathcal{H}$ with $\{x, y\} \subseteq H$.*

Proposition 3.12. *Every matroid of rank 3 is CI-compliant, and hence also AK-compliant.*

Proof. Clearly, it is enough to prove that, for every matroid (Q, r) of rank 3 and for every pair (A, B) of subsets of Q, there exists a matroid (Qx_o, r) of rank 3 extending (Q, r) such that x_o is a common information for the pair (A, B). Obviously, it is enough to prove the result for simple matroids and for pairs (A, B) of hyperplanes. Simple matroids of rank 3 are paving. Let $\mathcal{M}$ be a paving matroid of rank 3 on Q and let (H_1, H_2) be a pair of distinct hyperplanes of $\mathcal{M}$. If there exists $x_o \in H_1 \cap H_2$, then x_o is a common information for the pair (H_1, H_2). Otherwise, take $x_o \notin Q$ and consider the family $\mathcal{H}'$ of subsets of Qx_o formed by all hyperplanes of $\mathcal{M}$ other than H_1, H_2 together with H_1x_o, H_2x_o, and all pairs xx_o with $x \in Q \setminus (H_1 \cup H_2)$. It is easy to prove that $\mathcal{H}'$ satisfies the conditions in Lemma 3.11, and hence it is the family of hyperplanes of a paving matroid $\mathcal{M}'$ of rank 3 on Qx_o. Moreover, it is obvious that $\mathcal{M}'$ extends $\mathcal{M}$ and x_o is a common information for the pair (H_1, H_2). □

3.5 Minors of CI-compliant polymatroids

We give here some interesting results about the common information property and how it behaves with respect to minors. In a later section, we will look at optimizations of the CI property as well as some other such tools.

Lemma 3.13. *Let $\mathcal{S} = (Q, f)$ be a polymatroid, $A, B \subseteq Q$ and $X, Y \subseteq Q \setminus AB$. Let $\mathcal{T} = (Qx_0, f)$ be an extension of $\mathcal{S}$ where x_0 is a common information of (XA, YA). Then $\mathcal{T}/A\backslash B$ is an extension of $\mathcal{S}/A\backslash B$ where x_0 is a common information of X, Y.*

Proof. Since x_0 is a common information of (XA, YA) in $\mathcal{T}$, we have that

$$f(x_0) = f(XA) + f(YA) - f(XYA). \tag{3.1}$$

Let $Q' = Q \setminus AB$. Since $\mathcal{T}$ is an extension of $\mathcal{S}$, $\mathcal{T}/A\backslash B$ is an extension of $\mathcal{S}/A\backslash B$. We call them $\mathcal{T}' = (Q'x_0, f')$ and $\mathcal{S}' = (Q', f')$, respectively. Now, we have to prove that x_0 is a common information of X, Y in $\mathcal{T}'$. Notice that

$$\begin{aligned} f'(x_0|X) &= f'(x_0X) - f'(X) = f(x_0XA) - f(A) - f(XA) + f(A) \\ &= f(x_0XA) - f(XA) = 0. \end{aligned}$$

Following an analogous argument, we obtain that $f'(x_0|Y) = 0$. Combining (3.1), the fact that $f(x_0|XA) = f(x_0|YA) = 0$, and submodularity of f we have that

$$f(x_0) = f(XAx_0) + f(YAx_0) - f(XYAx_0) \geq f(Ax_0),$$

so $f(x_0) = f(Ax_0)$. Finally, observe that

$$\begin{aligned} f'(X) + f'(Y) - f'(XY) &= f(XA) - f(A) + f(YA) - f(A) - f(XYA) + f(A) \\ &= f(XA) + f(YA) - f(XYA) - f(A) \\ &= f(x_0) - f(A) = f(Ax_0) - f(A) = f'(x_0), \end{aligned}$$

and hence, x_0 is a common information of X, Y in $\mathcal{T}'$. □

Lemma 3.14. *Minors of 1-CI-compliant polymatroids are also 1-CI-compliant.*

Proof. Let $\mathcal{S}$ be a 1-CI-compliant polymatroid on Q, and let $\mathcal{S}'$ be a minor of $\mathcal{S}$. We can assume that $\mathcal{S}' = \mathcal{S}/A\backslash B$ for some $A, B \subseteq Q$, and the ground set of $\mathcal{S}'$ is $Q' = Q \smallsetminus AB$. In order to show that $\mathcal{S}'$ is 1-CI-compliant, we need to prove that for every $X, Y \subseteq Q'$ there is an extension of $\mathcal{S}'$ on $Q'x_0$ where x_0 is a common information of (X, Y).

Since $\mathcal{S}$ is 1-CI-compliant, there is an extension $\mathcal{T}$ on Qx_0 where x_0 is a common information of (XA, YA). By Lemma 3.13, $\mathcal{T}' = \mathcal{T}/A\backslash B$ is an extension of $\mathcal{S}'$ in which x_0 is a common information of X, Y. □

In the case of 1-AK-compliant polymatroids, we do not know if the analogous result holds. The following result generalizes the above to an arbitrary depth k of CI compliance.

Lemma 3.15. *Minors of k-CI-compliant polymatroids are also k-CI-compliant.*

Proof. The proof is straightforward from Lemmas 3.13 and 3.14. Let $\mathcal{S} = (Q, f)$ be a k-CI-compliant polymatroid for some $k > 0$. Let $\mathcal{S}'$ be a minor of $\mathcal{S}$. Assume that $\mathcal{S}' = \mathcal{S}/A \setminus B$ for some $A, B \subseteq Q$ with ground set $Q' = Q \smallsetminus AB$. In order to prove that $\mathcal{S}'_0 = \mathcal{S}'$ is k-CI-compliant, we need to show that for every sequence of subsets $(X_{i0}, X_{i1})_{1\leq i\leq k}$ with $X_{i0}, X_{i1} \subseteq Q'x_1 \dots x_{i-1}$ for $1 \leq i \leq k$ there is a sequence of polymatroids $\mathcal{S}'_1, \dots, \mathcal{S}'_k$ in which $\mathcal{S}'_i$ is an extension of $\mathcal{S}'_{i-1}$ with x_i being a common information of the pair (X_{i0}, X_{i1}).

Since $\mathcal{S}_0 = \mathcal{S}$ is k-CI-compliant, for every sequence of sets $(X_{i0}A, X_{i1}A)_{1\leq i\leq k}$ with $X_{i0}, X_{i1} \subseteq Q'x_1 \dots x_{i-1}$ there is a corresponding sequence of polymatroids $\mathcal{S}_1, \dots, \mathcal{S}_k$ each defined on the ground set $Qx_1, \dots, Qx_1 \dots x_k$ such that each $\mathcal{S}_i$ is an extension of $\mathcal{S}_{i-1}$, for $1 \leq i \leq k$.

By Lemma 3.13, the $\{\mathcal{S}_i/A \setminus B\}_{1\leq i\leq k}$ is a sequence of extensions of $\mathcal{S}'$ that satisfies the conditions stated above. □

An immediate consequence of this then is the following more general result.

Corollary 3.16. *Minors of CI-compliant polymatroids are also CI-compliant.*

3.6 LP for Algebraic Matroids

3.6.1 Generalizations of the Ingleton-Main Lemma

Ingleton and Main presented in [62] a necessary condition for a matroid to be algebraic. They showed that, in a fully algebraic matroid of rank at least 4, if there are three pairwise but not all coplanar lines, then all three lines have a common intersection. Using this, they proved that the Vámos matroid is not algebraic. Later, Lindström [74] generalised this result to the following theorem and removed the restriction to lines, generalising it to flats. By doing this he was able to demonstrate the existence of an infinite class of non-algebraic matroids.

Theorem 3.17 ([74])**.** *Let π_1, π_2 and π_3 be three flats of an algebraically closed combinatorial geometry over a field $\mathbb{K}$ such that $r(\pi_1 \vee \pi_2 \vee \pi_3) = r \geq 3$, $r(\pi_i \vee \pi_j) = r - 1$ $(1 \leq i < j \leq 3)$ and $r(\pi_i) = r - 2$ $(1 \leq i \leq 3)$. Then $\pi_1 \wedge \pi_2 = \pi_1 \wedge \pi_3 = \pi_2 \wedge \pi_3$ and the rank of this flat is $r - 3$.*

From theorem 3.17, we can define a linear programming problem that checks for polymatroid extensions for algebraic matroid. That is, let $\mathcal{M} = (Q, r)$ be an algebraic matroid and let U, V, and W be flats of $\mathcal{M}$ such that:

1. $r(U) = r(V) = r(W) = l \geq 2$,
2. $r(UV) = r(UW) = r(VW) = l + 1$,
3. $r(UVW) = l + 2$.

Then there exists a set X and a matroid extension $\mathcal{M}' = (QX, r)$ of $\mathcal{M}$ satisfying

1. $r(X) = l - 1$,
2. $r(UX) = r(VX) = r(WX) = l$.

In a related result, Dress and Lovasz [46] showed the following.

Theorem 3.18 ([46])**.** *Let $\mathcal{M}$ be a full algebraic matroid of finite rank and let U and V be two flats in $\mathcal{M}$. Then there exists a flat $T \subseteq U$ such that for each flat $W \subseteq U$,*

$$r(VW) - r(V) = r(VTW) - r(VT).$$

One can define a linear programming problem from this result as well that could also be useful in finding non-algebraic matroids.

3.6.2 LP programs

Below, we give a more formal description of the linear programming problems mentioned above.

Linear Programming Problem 3. Given a matroid $\mathcal{M} = (Q, r)$, $\ell \geq 1$, and three flats $A_1, A_2, A_3 \subseteq Q$ satisfying $r(A_I) = \ell + |I|$ for every nonempty set $I \subseteq \{1, 2, 3\}$, determine if there is a polymatroid (Qx_o, r) extending $\mathcal{M}$ such that $r(x_0) = \ell$ and $r(A_i x_0) = \ell + 1$ for every $i \in \{1, 2, 3\}$.

Linear Programming Problem 4. Given a matroid $\mathcal{M} = (Q, r)$, and two flats $A, B \subseteq Q$, determine if there is a polymatroid (Qx_o, r) extending $\mathcal{M}$ such that $r(Ax_0) = r(A)$ and

$$r(BC) - r(B) = r(BCx_0) - r(Bx_0)$$

for every flat $C \subseteq U$.

3.7 Optimizing LP techniques

In general, the number of equations for each of the LP problems we discussed above is exponential in n. Indeed, in order to guarantee that a vector in $\mathbb{R}^{2^Q}$ corresponds to the rank function of a polymatroid, we need to force monotonicity and submodularity for subsets of Q. Previous works on combinatorial optimization noticed that the number of conditions can be reduced considerably, by just considering inequalities for particular families of subsets. An example is the following theorem where it is shown that checking if a given function over a set is submodular can be done in a more systematic, non-naive way.

Theorem 3.19. *[100, Thm. 44.1] A set function r on Q is submodular if and only if*

$$r(U \cup s) + r(U \cup t) \geq r(U) + r(U \cup \{s, t\})$$

for each $U \subseteq Q$ and distinct $s, t \in Q \setminus U$.

This result, coupled with a similar reduction on the number of inequalities needed to determine monotonicity, brought down the number of inequalities to be checked from 2^{2n+1} to $n + \binom{n}{2}2^{n-2}$, which is still exponential in n [112]. This takes on greater significance when dealing with sets of size $n \geq 11$ as it means the computation may still not be fast enough, especially on conventional computers.

In order to restrict searches to polymatroids that satisfy the Ingleton inequality, Guillé, Chan and Grant [57] optimized the corresponding LP problem by finding a smaller subset of inequalities that guarantee the resulting polymatroid is Ingleton-compliant. In particular, they showed that, given a matroid with ground set Q, it is enough to check Ingleton-compliance using sets $A, B, C, D, N \subseteq Q$ where $A \cup N, B \cup N, C \cup N$ and $D \cup N$ form the 4 sets in the inequality, A, B, C, D, N are disjoint and A, B, C, D are non-empty; thereby considerably reducing the number of inequalities to be checked from 16^n to $6^n/4 - O(5^n)$.

Notice that if the number of variables is high and the computational cost of the full LP program is too high, it is also worth to carefully select a smaller set of inequalities of the LP program in order to obtain a sub-optimal lower bound [38].

3.7.1 CI and AK

In our LP problems for checking the representability of matroids using CI and AK properties, we applied the simplification in Theorem 3.19, as well as the results presented in this section.

We observe that while our result would see much use in determining non-representable matroids, its application in secret sharing is limited to only bounds on the information ratio of secret sharing schemes for matroid and polymatroid ports and not for other types of access structures like graph-based access structures or some access structures on small participants. This is due to the fact that we take into account properties that can be derived from (poly)matroids and not necessarily from other combinatorial structures.

Lemma 3.20. *Let $A \subseteq U \subseteq Q$ and $B \subseteq V \subseteq Q$ where U and V are flats and $r(A) = r(U)$ and $r(B) = r(V)$. Then there is a common information for (A, B) if and only if there is a common information for (U, V).*

Proof. Suppose x_0 is a common information for (A, B). Since $r(A : B) = r(x_0)$, $r(A) = r(U)$ and $r(B) = r(V)$, we have that

$$r(U : V) \geq r(A : B) = r(U) + r(V) - r(AB) \geq r(U : V).$$

This implies $r(U : V) = r(x_0)$. Now,

$$r(x_0|U) = r(Ux_0) - r(U) = r(AUx_0) - r(U) = r(AU) - r(U) = 0.$$

Same thing holds for $r(x_0|V)$. Hence, $x_0 = CI(U, V)$.

For the other direction, suppose x_1 is a common information for (U, V). We again have that

$$r(x_1) = r(U : V) \leq r(U) + r(V) - r(AB) = r(A : B) \leq r(U : V) = r(x_1),$$

which also implies $r(A : B) = r(x_1)$. Also,

$$r(U) = r(A) \leq r(Ax_1) \leq r(Ux_1) = r(U) = r(A).$$

Which implies $r(Ax_1) = r(A)$. Applying same argument to B, V and x_1 we have that $r(Bx_1) = r(B)$, completing the proof. □

Lemma 3.21. *Let $\mathcal{S} = (Q, r)$ be a polymatroid and let $U, V \subseteq Q$. If (U, V) is a modular pair of flats, then there exists an extension (Qx_0, r) such that x_0 is a common information for (U, V).*

Proof. Let $x_0 = U \cap V$. Since U and V are modular,

$$r(x_0) = r(U \cap V) = r(U) + r(V) - r(UV).$$

Also, $r(U \cap V|U) = r(U \cap V|V) = 0$. Hence, x_0 is a common information for (U, V). □

For the Ahlswede-Körner information we start with the following simple result.

Lemma 3.22. *Let $U, V, Z \subseteq Q$ be such that $r(U|Z) = r(V|Z) = 0$. Then there exists an extension $\mathcal{S}' = (Qz_0, r)$ such that z_0 is an AK information for (U, V, Z).*

Proof. Since $r(U|Z) = r(V|Z) = 0$, then we have that $r(UV|Z) = 0$ as well. Now, if we set $z_0 = UV$ we see that the AK axioms are all satisfied. Hence, UV is an AK information for (U, V, Z). □

One more result which will play a role in this section is Proposition 3.15 of [49]. We reproduce it here.

Proposition 3.23. *Let (Q, f) be a polymatroid and let $U, V, Z \subseteq Q$. Let $x_0 \subseteq Q$ be a common information for the pair (UV, Z). Then x_0 is an AK-information for the triple (U, V, Z). As a consequence, every polymatroid satisfying the common information property satisfies the AK-information property, too.*

Combining these, we have the following optimization for the Ahlswede-Körner information.

Theorem 3.24. *Let $\mathcal{S} = (Q, r)$ be a polymatroid and let $U, V, Z \subseteq Q$. If any of the following conditions hold, then there is an extension (Qz_0, r) of $\mathcal{M}$ such that z_0 is an AK information for (U, V, Z).*

(i) UV and Z are a modular pair of sets.

(ii) $r(UZ) = r(Z)$ and $r(VZ) = r(Z)$.

Proof. Consequence of Proposition 3.23 via Lemma 3.21 for item (i) and Lemma 3.22 for item (ii). □

3.7.2 Zhang-Yeung inequality

We conclude this section with a minor result on the optimization of the Zhang-Yeung inequality. In order to reduce the notaion, we define the following function. Given a polymatroid (Q, r) and $A, B, C, D \subseteq Q$, we define

$$\begin{aligned}\mathcal{ZY}(A, B, C, D) = {} & 3r(AB) + 3r(BC) + 3r(AC) + r(AD) + r(BD) \\ & - 2r(A) - 2r(B) - r(C) - 4r(ABC) - r(CD) - r(ABD). \end{aligned} \tag{3.2}$$

As a consequence of the Zhang-Yeung inequality, if (Q, r) is an entropic polymatroid, then $\mathcal{ZY}(A, B, C, D) \geq 0$ for every $A, B, C, D \subseteq Q$.

A careful study of (3.2) would reveal that the sets A and B mirror each other in the inequality, i.e,

$$\mathcal{ZY}(A, B, C, D) = \mathcal{ZY}(B, A, C, D),$$

and we make use of this symmetry in the proof of the following proposition.

Proposition 3.25. *Let $\mathcal{M} = (Q, r)$ be a matroid of rank d. For any four subsets A, B, C, D of Q, if any of the following holds, then the Zhang-Yeung inequality (3.2) is satisfied:*

(i) $r(AB) = r(A)$ *or* $r(AB) = r(B)$.

(ii) $r(AC) = r(A)$ *and* $r(BC) = r(B)$.

(iii) $r(ABC) = r(C)$.

(iv) $r(X) = 0$ *or* $r(X) = d$ *for any* $X \in \{A, B, C, D\}$.

(v) $r(AB) = r(X) = d$ *for any* $X \in \{AC, AD, BC, BD, CD\}$.

Proof. In this proof we employ the conditional mutual information and conditional entropy where we use the submodularity and monotonicity properties of the Shannon entropy. Also, in order to reduce the length of the proof, we use the notation $\mathcal{ZY}(A, B, C, D)\big|_{cond}$ to express the case of $\mathcal{ZY}$ restricted to when the condition *cond* is satisfied.

(i)

$$\begin{aligned}\mathcal{ZY}(A, B, C, D)\Big|_{r(AB)=r(B)} &= r(B) + 3r(AC) + r(AD) - 2r(A) - r(C) - r(BC) - r(CD) \\ &= r(B : C|A) + r(C : D|A) + r(A|C) \geq 0.\end{aligned}$$

The proof for $r(AB) = r(A)$ is analogous.

(ii)

$$\begin{aligned}\mathcal{ZY}(A, B, C, D)\Big|_{r(AC)=r(A);r(BC)=r(B)} &= r(A) + r(B) + r(AD) + r(BD) - r(C) - r(AB) - r(CD) - r(ABD) \\ &= r(A : B|CD) + r(A : B|C) \geq 0.\end{aligned}$$

(iii)

$$\begin{aligned}\mathcal{ZY}(A, B, C, D)\Big|_{r(ABC)=r(C)} &= 3r(AB) + r(C) + r(AD) + r(BD) - 2r(A) - 2r(B) - r(CD) - r(ABD) \\ &= r(A : D|B) + r(D : C|A) + r(A|B) + r(B|A) \geq 0.\end{aligned}$$

(iv)

$$\begin{aligned}\mathcal{ZY}(A, B, C, D)\Big|_{r(A)=d} &= 3r(BC) + r(BD) - 2r(B) - r(C) - r(CD) \\ &\geq r(C : D|B) + r(B|C) + r(C|B) \geq 0.\end{aligned}$$

Observe that in the first inequality, we use that $r(BCD) \geq r(CD)$. The proof for $r(B) = d$ follows with $r(ACD) \geq r(CD)$.

$$\begin{aligned}\mathcal{ZY}(A,B,C,D)\Big|_{r(A)=0} &= r(B)+2r(C)+r(D)-r(BC)-r(CD)\\ &= r(B:C)+r(C:D)\geq 0.\end{aligned}$$

The case $r(B)=0$ is analogous.

$$\begin{aligned}\mathcal{ZY}(A,B,C,D)\Big|_{r(C)=d} &= 3r(AB)+r(AD)+r(BD)-2r(A)-2r(B)-r(ABD)\\ &= r(A:D|B)+r(A|B)+r(B|A)+r(D|A)\geq 0.\end{aligned}$$

$$\begin{aligned}\mathcal{ZY}(A,B,C,D)\Big|_{r(C)=0} &= r(A)+r(B)+r(AD)+r(BD)-r(AB)-r(D)-r(ABD)\\ &= r(A:B|D)+r(A:B)\geq 0.\end{aligned}$$

$$\begin{aligned}\mathcal{ZY}(A,B,C,D)\Big|_{r(D)=d} &= 3r(AB)+3r(BC)+3r(AC)-2r(A)-2r(B)-r(C)-4r(ABC)\\ &= 2r(C:B|A)+r(A:C|B)+r(A:B|C)\geq 0.\end{aligned}$$

$$\begin{aligned}\mathcal{ZY}(A,B,C,D)\Big|_{r(D)=0} &= 2r(AB)+3r(BC)+3r(AC)-r(A)-r(B)-2r(C)-4r(ABC)\\ &= 2r(B:A|C)+r(B:C|A)+r(A:C|B)\geq 0.\end{aligned}$$

(v)

$$\begin{aligned}\mathcal{ZY}(A,B,C,D)\Big|_{r(AB)=r(AC)=d} &= 3r(BC)+r(AD)+r(BD)+d-2r(A)-2r(B)-r(C)-r(CD)\\ &\geq r(C:D|B)+r(B|C)+r(C|B)+r(D|A)+d-r(A)\geq 0.\end{aligned}$$

In the first inequality we use the fact that $r(BCD)\geq r(CD)$. The case $r(AB)=r(BC)=d$ follows with $r(ACD)\geq r(CD)$.

$$\begin{aligned}
&\mathcal{ZY}(A,B,C,D)\Big|_{r(AB)=r(AD)=d} \\
&\quad = 3r(BC) + 3r(AC) + r(BD) - d - 2r(A) - 2r(B) - r(C) - r(CD) \\
&\quad \geq r(C:D|B) + r(A:B|C) + 2r(C|A) + r(C|B) \geq 0.
\end{aligned}$$

In the first inequality we use the fact that $r(BCD) \geq r(CD)$. The case $r(AB) = r(BD) = d$ follows with $r(ACD) \geq r(CD)$.

$$\begin{aligned}
&\mathcal{ZY}(A,B,C,D)\Big|_{r(AB)=r(CD)=d} \\
&\quad = 3r(BC) + 3r(AC) + r(AD) + r(BD) - 3d - 2r(A) - 2r(B) - r(C) \\
&\quad = r(A:B|C) + r(C:D|A) + r(C:D|B) + r(C|A) + r(C|B) \geq 0.
\end{aligned}$$

□

Chapter 4

Classification of Matroids

4.1 Introduction

The contents of this chapter cover parts of [10] that relate to results obtained by the application of the common information and AK-information properties to the problem of matroid classification as discussed in the previous chapter. In this chapter and onwards, we will sometimes denote matroids of rank r on n points as (r, n) matroids, borrowing the language of [28].

We start with 8-point matroids. From the 5 non-linear Ingleton-compliant matroids on 8 points [87] (P_1, P_2', P_2'', P_3 and L_8'), we use the matrix representation of folded-linear matroids to show that only P_3 and L_8' are folded linear, thereby completing the classification of 8-point matroids in this regard. This result means that both matroids are the smallest non-linear matroids that are folded linear (the smallest found prior to now is the non-Pappus matroid, which is a 9-point matroid [91]). We also show that matroids on 8 points are representable over skew fields if and only if they are folded linear. A similar result we show is that, for matroids on 8 points, folded linear implies algebraicity.

For 9-point matroids, we present three new families of Ingleton-compliant non folded-linear $(5, 9)$ matroids. The first family is perhaps the most interesting as it contains the Tic-Tac-Toe matroid, a prime candidate for the solution of the question of whether duality preserves algebraicity. We call matroids in this family TTT matroids (Section 4.3). Similarly to what was shown for the 39 non-Ingleton-compliant $(4, 8)$ matroids [87], we show that TTT matroids can be seen to derive from the Tic-Tac-Toe matroid, being the smallest in terms of number of circuit-hyperplanes. These matroids are all sparse-paving non-1-CI matroids, and hence, are not folded linear. They satisfy the Dress-Lovasz and Ingleton-Main extensions [28] at arbitrary depths. We also extend this family to those with more than 9 points.

In addition to studying the TTT matroids, we also study their duals. We show that they are not almost entropic by 3-AK. This result uses two key facts: one being that duals of $(5, 9)$ TTT matroids are not 3-AK, and the other that the class of almost entropic matroids is minor-closed [83].

The second family of Ingleton-compliant non folded-linear 9-point matroids we found (Section 4.5.1) is made up of some non sparse-paving matroids that are not 1-CI. These

matroids are similar to the TTT matroids. Their duals fail AK at depth 3, and hence, are not almost entropic.

Working with matroids on 9 points, we found that we needed more tools to supplement the ones we had already. For this, we turned to the matroid intersection properties that had been studied in the past [3, 8, 9]. These intersection properties are satisfied by all linearly representable matroids and were designed to be used in 1 step, i.e., checking to see if the matroid admits an extension with certain properties. However, we show in this chapter that they can be extended to n depths, for some integer $n \geq 1$ (Section 4.4).

With these recursive definitions of the intersection properties, we found our third family of Ingleton-compliant non folded-linear $(5, 9)$ matroids (Section 4.5.2). Matroids in this family satisfy CI, AK, and the three intersection properties at depth 1. All the matroids here fail the intersection properties at depth 2, and hence, are not linear. Also, we were able to confirm that many of them fail CI at depth 2, and hence, are not folded linear. We present these matroids in Table 4.2. We should note that, unlike the other two families, this list is not exhaustive as we were not able to find all the matroids in this family due to time constraints.

We conclude this chapter with a discussion on the results of [28] and how it relates to the matroids we studied (Section 4.6). Two results to highlight about this section are the numbers of 8- and 9-point matroids we can confirm to not be almost entropic. In the case of 8-point matroids, there are at least 39 matroids that are not almost entropic and three with an undetermined status (P_1, P_2' and P_2'').

There are at least 27,137 non almost entropic $(5, 9)$ matroids based on the fact that these matroids are not Ingleton-compliant. Same applies to their duals. But in addition to their duals, there are 288 Ingleton-compliant $(4, 9)$ matroids we can also confirm to not be almost entropic. These are the duals of the TTT matroids and the matroids in Section 4.5.1. They are all non-3-AK matroids. Hence, we can say that there are at least 27,425 $(4, 9)$ matroids that are not almost entropic.

4.2 Matroids on 8 Points

The matroids $AG(3, 2)$, $AG(3, 2)'$, F_8, Q_8, V_8 (Vámos matroid), P_8, and L_8 appearing in this section and in Section 5.4 are described in the Appendix of Oxley's book [91]. Given a sparse-paving matroid $\mathcal{M}$, a new such matroid $\mathcal{M}'$ can be obtained by *relaxing* one of its circuit-hyperplanes, that is, by transforming it into a basis. In that situation, $\mathcal{M}'$ is called a *relaxation* of $\mathcal{M}$.

4.2.1 Matroids that are not Ingleton-compliant

Mayhew and Royle [87] provided a comprehensive list of matroids on up to 9 points, specifying how many of them are simple, paving, or sparse paving. They also presented the list of all 44 non-linear matroids on 8 points, which are sparse paving and of rank 4. Since every matroid on at most 7 points is linear, those are the smallest non-linear matroids. Exactly 39 of them are not Ingleton-compliant, which implies by Theorem 3.10 that they are neither almost entropic nor algebraic. Those 39 matroids, which include F_8 and Q_8, are relaxations of the binary affine cube $AG(3, 2)$, with $AG(3, 2)'$ and the

Vámos matroid V_8 the ones among them with, respectively, most and fewest circuit-hyperplanes. The matroids in [87] are named according to the database provided by the same authors in [99]. In this thesis we follow the same notation.

4.2.2 Folded-Linear Matroids

The 5 remaining non-linear matroids on 8 points are P_1, P_2', P_2'', and P_3, which are relaxations of P_8, and a relaxation L_8' of L_8. Take $Q = \{0, 1, \ldots, 7\}$ as the ground set of those sparse-paving matroids. The circuit-hyperplanes of P_8 are

$$0127, 0136, 0235, 1234, 0456, 1457, 2467, 3567, 0347, 1256,$$

while the ones of L_8 are

$$0246, 1357, 0156, 2347, 0127, 3456, 0457, 1236.$$

The matroid P_1 is obtained from P_8 by relaxing the circuit-hyperplane 3567 of P_8. The relaxation of 0347 from P_1 gives the matroid P_2', while P_2'' is obtained from P_1 by relaxing 1256. The relaxation of both 0347 and 1256 from P_1 produces the matroid P_3. Finally, the matroid L_8' is obtained from L_8 by relaxing the circuit-hyperplane 0457.

By applying Linear Programming Problem 1 to those five non-linear matroids, we found that they are 1-CI-compliant, and hence also 1-AK-compliant by Proposition 3.7. We explored the possibility that some of them were folded-linear matroids. To that end, we combined the technique to find linear representations of matroids presented in [91, Section 6.4] with the tools for folded-linear matroids given in [14] and we concluded that only P_3 and L_8' are folded-linear matroids.

Theorem 4.1. *The smallest non-linear matroids that are folded linear are precisely P_3 and L_8'.*

Before proving Theorem 4.1, we describe how to use the techniques from [14, 91] to that end. Unless otherwise stated, the blocks in the matrices appearing in this section are square matrices of size ℓ. We use capital letters to represent them. As usual, the identity and zero matrices are denoted by I and 0, respectively.

Consider a matroid $\mathcal{M} = (Q, r)$ of rank m on n points, a field $\mathbb{F}$, and a positive integer ℓ. Assume that $Q = \{0, 1, \ldots, n-1\}$ is the ground set of $\mathcal{M}$. Every $\mathbb{F}$-linear representation of the polymatroid $(Q, \ell r)$ is called an $(\mathbb{F}, \ell)$-*linear representation of* $\mathcal{M}$, and it is determined by a block matrix over $\mathbb{F}$ of the form

$$B = \begin{pmatrix} B_{0,0} & \cdots & B_{0,n-1} \\ \vdots & & \vdots \\ B_{m-1,0} & \cdots & B_{m-1,n-1} \end{pmatrix}, \tag{4.1}$$

where each block $B_{i,j}$ is a square matrix of size ℓ. If V_i is the vector subspace of $\mathbb{F}^{\ell m}$ spanned by the columns in the i-th block-column, then $(V_i)_{i \in Q}$ is an $\mathbb{F}$-linear representation of the polymatroid $(Q, \ell r)$. By the next result, there exists such a matrix in which every block is either invertible or zero.

Lemma 4.2. *Suppose that $A = \{0, 1, \ldots, m-1\}$ is a basis of $\mathcal{M}$. For each $j = m, \ldots, n-1$, consider the fundamental circuit $C(j, A)$, that is, the only circuit contained in $A \cup j$. Then there exists a block matrix of the form*

$$\left(\begin{array}{ccc|ccc} I & \cdots & 0 & B_{0,m} & \cdots & B_{0,n-1} \\ \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \cdots & I & B_{m-1,m} & \cdots & B_{m-1,n-1} \end{array}\right), \tag{4.2}$$

providing an $(\mathbb{F}, \ell)$-linear representation of $\mathcal{M}$. Furthermore, in every such representation, each block $B_{i,j}$ with $j \geq m$ is invertible if $i \in C(j, A)$ and it is zero otherwise.

Proof. If B', a block matrix of the form (4.1), is an $(\mathbb{F}, \ell)$-linear representation of $\mathcal{M}$, then the submatrix T formed by the block-columns corresponding to the basis A is invertible. Clearly, $B = T^{-1}B'$ is an $(\mathbb{F}, \ell)$-linear representation of $\mathcal{M}$ of the form (4.2). Consider $j \geq m$. Without loss of generality, suppose that $C(j, A) = \{0, \ldots, s-1, j\}$ for some $s \leq m$. Since the submatrix of B formed by the block-columns corresponding to $C(j, A)$ has rank ℓs, it is clear that $B_{i,j} = 0$ if $s \leq i \leq m-1$. If, otherwise, $0 \leq i \leq s-1$, the rank of the submatrix formed by the block-columns corresponding to $C(j, A) \setminus i$ equals ℓs, which implies that $B_{i,j}$ is invertible. □

Following [14], we are going to use two operations on block matrices representing folded-linear matroids. Namely, *block-column scaling* and *row-block scaling*.

Lemma 4.3 ([14] Proposition 2.12)**.** *Let $\mathcal{M}$ be an ℓ-folded-linear matroid represented by a block matrix B of the form* (4.1) *and let G be an invertible $\ell \times \ell$ matrix. Then, for each $i = 0, \ldots, m-1$, the matrix*

$$\begin{pmatrix} B_{0,0} & \cdots & B_{0,n-1} \\ \vdots & & \vdots \\ GB_{i,0} & \cdots & GB_{i,n-1} \\ \vdots & & \vdots \\ B_{m-1,0} & \cdots & B_{m-1,n-1} \end{pmatrix}$$

is also an $(\mathbb{F}, \ell)$-linear representation of $\mathcal{M}$, and the same applies to the matrix

$$\begin{pmatrix} B_{0,0} & \cdots & B_{0,j}G & \cdots & B_{0,n-1} \\ \vdots & & \vdots & & \vdots \\ B_{m-1,0} & \cdots & B_{m-1,j}G & \cdots & B_{m-1,n-1} \end{pmatrix}$$

for each $j = 0, \ldots, n-1$.

Block scaling can help significantly in simplifying the study of $(\mathbb{F}, \ell)$-linear representations. By the following lemma, we can assume that several blocks $B_{i,j}$ in (4.2) equal the identity matrix. It is a straightforward generalization of [91, Theorem 6.4.7], the analogous result for linear representations of matroids.

Lemma 4.4. *Let $\mathcal{M}$ be an ℓ-folded $\mathbb{F}$-linear matroid that admits an $(\mathbb{F}, \ell)$-representation B' of the form* (4.2)*. Take $V = \{0, \ldots, m-1\}$ and $W = \{m, \ldots, n-1\}$. Consider the bipartite graph G with set of vertices $V \cup W$ such that $(i, j) \in V \times W$ is an edge if and only if $B'_{i,j} \neq 0$. Let E be the set of edges of a maximal acyclic subgraph of G. Then*

a sequence of block scalings provides an $(\mathbb{F},\ell)$*-representation* B *of the form* (4.2) *such that* $B_{i,j} = I$ *if* $(i,j) \in E$.

Proof. Adapt the proof of [91, Theorem 6.4.7] in the obvious way. □

The graph G is connected for many matroids, and in that case we can choose any spanning tree of G and we can assume that the $n-1$ blocks $B_{i,j}$ with $j \geq m$ corresponding to its edges are equal to I. We are now ready to prove Theorem 4.1.

Proof of Theorem 4.1. Let $\mathcal{M}$ be one of the matroids P_1, P_2', P_2'', P_3 and suppose that it is an ℓ-folded $\mathbb{F}$-linear matroid for some field $\mathbb{F}$ and some positive integer ℓ. Since 0123 is a basis, by Lemmas 4.2 and 4.4, we can assume that $\mathcal{M}$ admits an $(\mathbb{F},\ell)$-linear representation of the form

$$\left(\begin{array}{cccc|cccc} I & 0 & 0 & 0 & 0 & I & I & I \\ 0 & I & 0 & 0 & I & 0 & I & A \\ 0 & 0 & I & 0 & I & B & 0 & C \\ 0 & 0 & 0 & I & I & D & E & 0 \end{array}\right) \tag{4.3}$$

where all nonzero blocks are invertible. We next consider the circuit-hyperplanes 0456, 1457, and 2467. The submatrices corresponding to those sets are, respectively,

$$\begin{pmatrix} I & 0 & I & I \\ 0 & I & 0 & I \\ 0 & I & B & 0 \\ 0 & I & D & E \end{pmatrix}, \begin{pmatrix} 0 & 0 & I & I \\ I & I & 0 & A \\ 0 & I & B & C \\ 0 & I & D & 0 \end{pmatrix}, \text{ and } \begin{pmatrix} 0 & 0 & I & I \\ 0 & I & I & A \\ I & I & 0 & C \\ 0 & I & E & 0 \end{pmatrix}.$$

Each of these matrices has rank 3ℓ. Gaussian elimination transforms those matrices into

$$\begin{pmatrix} I & 0 & I & I \\ 0 & I & 0 & I \\ 0 & 0 & B & -I \\ 0 & 0 & 0 & DB^{-1}+E-I \end{pmatrix}, \begin{pmatrix} I & I & 0 & A \\ 0 & I & D & 0 \\ 0 & 0 & I & I \\ 0 & 0 & 0 & C-B+D \end{pmatrix}, \text{ and } \begin{pmatrix} I & I & 0 & C \\ 0 & I & E & 0 \\ 0 & 0 & I & I \\ 0 & 0 & 0 & A-I+E \end{pmatrix}.$$

Therefore,

$$D = (I-E)B, \tag{4.4}$$
$$C = B - D = EB, \tag{4.5}$$
$$A = I - E. \tag{4.6}$$

Since 3567 is a basis, the corresponding submatrix has full rank. Gaussian elimination on it yields

$$\begin{pmatrix} I & D & E & 0 \\ 0 & I & I & I \\ 0 & 0 & I & A \\ 0 & 0 & 0 & C-B+BA \end{pmatrix}.$$

By the previous equations, $C - B + BA = EB - BE$, and hence

$$EB \neq BE, \tag{4.7}$$

which is possible only if $\ell > 1$.

Clearly, the submatrix corresponding to the set 0347 has rank 3ℓ if and only if $C = A$. But $C \neq A$ because, otherwise, $B = E^{-1} - I$ by (4.5) and (4.6), and then $EB = BE$, a contradiction with (4.7). As a consequence, P_1 and P_2'' do not admit any $(\mathbb{F}, \ell)$-linear representation.

Similarly, the submatrix corresponding to 1256 has rank 3ℓ if and only if $D = E$. We claim that this is impossible and, as a consequence, P_2' is not a folded-linear matroid. Indeed, if $D = E$, and since $I - E = A$ by (4.6) and thus invertible, then $B = (I-E)^{-1}E$ by (4.4) and

$$(I - E)EB = (I - E)E(I - E)^{-1}E = E(I - E)(I - E)^{-1}E = E^2 = (I - E)BE,$$

which is a contradiction with (4.7).

Since both 1256 and 0347 are bases of P_3, it is still possible to find an $(\mathbb{F}, \ell)$-linear representation for it. If there exists such a representation, then the matrices corresponding to 0347 and 1256 have full rank, and hence the matrices $B - E^{-1} + I$ and $E - (I - E)B$ are invertible. After substituting A, C, and D in (4.3) according to (4.6), (4.5) and (4.4), the following plausible $(\mathbb{F}, \ell)$-linear representation for P_3 is obtained

$$\left(\begin{array}{cccc|cccc} I & 0 & 0 & 0 & 0 & I & I & I \\ 0 & I & 0 & 0 & I & 0 & I & I-E \\ 0 & 0 & I & 0 & I & B & 0 & EB \\ 0 & 0 & 0 & I & I & (I-E)B & E & 0 \end{array}\right). \tag{4.8}$$

As a matter of fact, if we take

$$B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } E = \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$$

it can be checked that it results in a $(GF(5), 2)$-linear representation for that matroid.

We next prove in a similar fashion that L_8' is also a folded-linear matroid. If this is the case, by Lemmas 4.2 and 4.4, there exists an $(\mathbb{F}, \ell)$-linear representation of the form

$$\left(\begin{array}{cccc|cccc} I & 0 & 0 & 0 & I & I & 0 & I \\ 0 & I & 0 & 0 & D & C & I & A \\ 0 & 0 & I & 0 & E & I & I & B \\ 0 & 0 & 0 & I & F & G & I & 0 \end{array}\right).$$

Proceeding in the same way as before, from the circuit-hyperplanes 0156, 0246, 1357, 2347, and 3456 we can conclude that

$$G = I, \quad F = D, \quad B = I, \quad A = D, \text{ and } \quad C = I - E + D.$$

Since 0457 is a basis, the corresponding submatrix

$$\begin{pmatrix} I & I & I & I \\ 0 & D & C & A \\ 0 & E & I & B \\ 0 & F & G & 0 \end{pmatrix} = \begin{pmatrix} I & I & I & I \\ 0 & D & I-E+D & D \\ 0 & E & I & I \\ 0 & D & I & 0 \end{pmatrix}$$

has full rank. By Gausian elimination, we obtain

$$\begin{pmatrix} I & I & I & I \\ 0 & I & D^{-1} & 0 \\ 0 & 0 & I - ED^{-1} & I \\ 0 & 0 & DED^{-1} - E & 0 \end{pmatrix},$$

hence $DED^{-1} - E$ has full rank. In particular, this implies that $\ell > 1$. In conclusion, if L'_8 is a folded-linear matroid, it admits an $(\mathbb{F}, \ell)$-linear representation of the form

$$\left(\begin{array}{cccc|cccc} I & 0 & 0 & 0 & I & I & 0 & I \\ 0 & I & 0 & 0 & D & I - E + D & I & D \\ 0 & 0 & I & 0 & E & I & I & I \\ 0 & 0 & 0 & I & D & I & I & 0 \end{array}\right) \tag{4.9}$$

with $DE \neq ED$ and $I - E + D$ invertible. Take i, with $i^2 = -1$. The choice

$$D = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } E = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

does result in a $(GF(5^2), 2)$-linear representation of L'_8. This can be checked by using a computer. □

4.2.3 Algebraic Matroids and Skew-Field Representable Matroids

There exist folded-linear matroids that are not algebraic [22], but none on 8 points.

Proposition 4.5. *Every folded-linear matroid on* 8 *points is algebraic.*

Proof. Since linear matroids are algebraic, we only need to consider P_3 and L'_8. Both are algebraic over all fields with finite characteristic [29, Example 35]. The result for P_3 was first proved by Lindström [72]. □

The notion of linear representations of matroids over fields can be extended to linear representations over skew-fields. Matroids that admit such a representation are said to be *linearly representable over a skew-field*, or *skew-field representable* for short. The relation between skew-field representable matroids and folded-linear matroids has been studied in [96, 109]. It is known that there exist folded-linear matroids that are not representable over any skew-field [96]. In the other direction, some connections have been made in [109]. We found that, for matroids with at most 8 points, these two classes of matroids coincide.

Proposition 4.6. *A matroid on at most* 8 *points is skew-field representable if and only if it is a folded-linear matroid.*

Proof. Every linearly representable matroid is also skew-field representable. Skew-field representable matroids are CI-compliant, so the 39 non-Ingleton compliant matroids discussed above are not representable over skew-fields. The techniques in Section 4.2.2 can also be adapted to representations over skew-fields. In particular, one can prove in that way that P_1, P'_2 and P''_2 are not skew-field representable. Moreover, the matrix (4.9)

provides a representation of L_8' over the quaternion division ring $\mathbb{R}(i,j,k)$ by taking $E = i$ and $D = j$. A representation of P_3 over the quaternion division ring is obtained from the matrix (4.8) by taking $B = k$ and $E = j$. □

Remark 4.7. The only matroids on 8 points for which it is not known whether they are algebraic, almost entropic, or entropic are P_1, P_2', and P_2''.

We can summarise the current classification of matroids on 8 points as follows. There are 44 matroids that are not linear (Section 4.2.1) and, among them, exactly two are folded linear (Theorem 4.1). Also, on 8 points, a matroid is skew-field representable if and only if it is a folded linear matroid (Proposition 4.6), and the folded linear ones are algebraic (Proposition 4.5). There are three matroids on 8 points for which it is not known whether they are algebraic, almost entropic, or entropic (Remark 4.7). A classification of these three matroids will conclude the characterization of algebraic, entropic, and almost entropic matroids on 8 points.

4.3 TTT Matroids

By taking into account the results in [43] about linear rank inequalities derived from the common information property, one may expect that there are Ingleton-compliant matroids that are not CI-compliant. As a consequence of the results in Sections 4.2.1 and 4.2.2, a matroid on 8 points is 1-CI-compliant if and only if it is Ingleton-compliant. Mayhew and Royle [87] found that every matroid on 9 points that is not Ingleton-compliant contains a minor on 8 points with the same property. By solving Linear Programming Problem 1 for many matroids on 9 points from the database [99], we found some Ingleton-compliant but not CI-compliant matroids having a special configuration. We discuss these matroids in this and the following sections.

We begin by describing the Tic-Tac-Toe matroid [3]. Consider the 9-point matroid whose circuit-hyperplanes are all sets of the form $a_1a_2a_3b_ic_i$ for $i \in \{1,2,3\}$, $c_1c_2c_3a_ib_i$ for $i \in \{1,2,3\}$, and $b_1b_2b_3a_ic_i$ for $i \in \{1,3\}$. This is the matroid given in Fig. 4.1 and it is called the Tic-Tac-Toe matroid. This is a sparse-paving rank-5 matroid that is not linearly representable. The make-up of its circuit-hyperplanes can be broken down further as follows.

Let $\{r_1, r_2, r_3\}$ and $\{l_1, l_2, l_3\}$ be the rows and columns of Fig. 4.1, respectively. We observe that every pair r_il_j for $i,j \in \{1,2,3\}$ forms a circuit-hyperplane except r_2l_2. This is the bipartite graph of Fig. 4.2.

We found that this configuration of its circuit-hyperplanes makes the Tic-Tac-Toe matroid non-CI-compliant. In our computations we found that for every pair of subsets that correspond to parallel lines in Fig. 4.1 it is not possible to find an extension of the Tic-Tac-Toe matroid in which the added element is the common information of this pair of lines. We formally define matroids with this configuration below.

Definition 4.8. Let $\mathcal{M}$ be a sparse-paving matroid with rank $r \geq 5$ and ground set Q. If there exist sets $C, r_1, r_2, r_3, l_1, l_2, l_3 \subseteq Q$ such that $|C| = r-5$, each of $r_1, r_2, r_3, l_1, l_2, l_3$ is a size-3 set disjoint from C with $|r_i \cap l_j| = 1$ and $r_i \cap r_j = \emptyset = l_i \cap l_j$ for $i,j \in \{1,2,3\}$, and each set Cr_il_j, for $i,j \in \{1,2,3\}$ is a circuit-hyperplane except Cr_2l_2, then $\mathcal{M}$ is said to have the *TTT configuration* and is called a *TTT matroid*.

Remark 4.9. Observe that since we restrict the TTT configuration to sparse-paving matroids, then we have that all r_i's and l_i's, for $i \in \{1,2,3\}$ are rank-3 flats and that $r(Cr_ir_j) = r(Cl_il_j) = r$ for $i,j \in \{1,2,3\}$. Also, while the Tic-Tac-Toe matroid only has as circuit-hyperplanes those mentioned in Def. 4.8, TTT matroids in general can have other circuit-hyperplanes in addition. Hence, we place no restrictions on sets not explicitly mentioned in Def. 4.8.

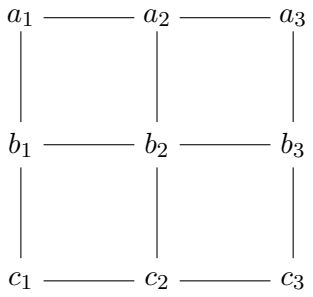


FIGURE 4.1: Tic-Tac-Toe Matroid

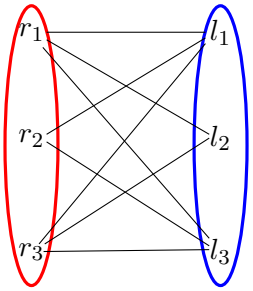


FIGURE 4.2: Bipartite Graph of Circuit-Hyperplanes of Tic-Tac-Toe

By doing an exhaustive search on 9-point matroids, we found all 181 sparse-paving $(5,9)$ TTT matroids with 10 of them being non-Ingleton-compliant matroids. While most of our results on these matroids are obtained computationally, it is possible to give a manual proof for some of them. We start with the fact that TTT matroids are not folded-linear matroids.

Matroid extensions are governed by what is called modular cuts (see Def. 2.17 and [91, Section 7.2]). This was used by Alfter and Hochstättler [3] to show that the Tic-Tac-Toe matroid does not satisfy the generalized Euclidean intersection property and hence is not linearly representable. Notice, however, that this is not enough to prove that it is not folded-linear.

4.3.1 TTT Matroids are not CI-compliant

To show that the Tic-Tac-Toe matroid, and indeed all TTT matroids, are not folded-linear matroids we can use the common information property. And since the CI property is also an extension property, albeit for polymatroids, we can use the same ideas as [3], but with caution. We need the following lemma.

Extending the notion of modular pairs in matroids, we say that two sets $A, B \subseteq Q$ are a modular pair of a polymatroid $\mathcal{S} = (Q, f)$ if $f(A) + f(B) = f(AB) + f(A \cap B)$.

Lemma 4.10. *Let $\mathcal{S} = (Q, f)$ be a polymatroid and let $A, B \subseteq Q$ be a modular pair. Let X_0 be such that $f(X_0|A) = f(X_0|B) = 0$. Then $f(X_0|A \cap B) = 0$.*

Proof. Since they are modular, $f(A \cap B) = f(A) + f(B) - f(AB)$. By submodularity, $f((A \cap B)X_0) \leq f(AX_0) + f(BX_0) - f(ABX_0) = f(A) + f(B) - f(AB) = f(A \cap B)$. Therefore, $f((A \cap B)X_0) = f(A \cap B)$. □

Theorem 4.11. *TTT matroids are non-CI-compliant.*

Proof. We prove this by contradiction. Let $y = r_2 \cap l_2$. Suppose $\mathcal{M}$ is 1-CI. Take the pair of flats (Cr_1, Cr_2). Then there exists a polymatroid extension (Qx_0, r) of $\mathcal{M}$ where x_0 is a common information of (Cr_1, Cr_2). Observe that

$$r(x_o) = r(Cr_1) + r(Cr_2) - r(Cr_1r_2) = r - 2 + r - 2 - r = r - 4,$$

and that $r(Cx_0) \geq r - 4$.

Let Γ be the family of subsets $A \subseteq Q$ for which $f(x_0|A) = 0$. Notice that Γ is monotone increasing. Since (Cr_1l_3, Cr_2l_3) and (Cr_1l_1, Cr_2l_1) are modular pairs of sets in Γ, Cl_3 and Cl_1 are in Γ by Lemma 4.10. Then Cr_3l_1, Cr_3l_3 are also in Γ and, applying Lemma 4.10, we get that $Cr_3 \in \Gamma$. Thus Cr_3l_2 is in Γ, and Cl_2 is in Γ by Lemma 4.10. Now, (Cr_2, Cl_2) is a modular pair, and hence, $Cy = Cr_2 \cap Cl_2$ is in Γ. Also, (Cy, Cr_1) is a modular pair. Therefore, $C \in \Gamma$ and $r(Cx_0) = r(C) = r - 5$, a contradiction. □

Proposition 4.12. *Ingleton-compliant 9-point TTT matroids are also 1-AK-compliant.*

The proof of the above result is computational and is therefore not shown. These matroids are also ZY-compliant matroids, i.e., they satisfy the Zhang-Yeung inequality. We note that while we are unable to say anything about the algebraicity of these matroids since they are 1-AK matroids, Bollen [28] has been able to determine that some of them are not algebraic over fields of characteristic 2. His results are discussed in Section 4.6 and also in Appendix A.1.

The family of TTT matroids on 9 points together forms a connected undirected graph. Also, if viewed as a directed graph (see Fig. 4.3), then there is a path from any of these matroids to the Tic-Tac-Toe matroid. In essence, this means that the Tic-Tac-Toe matroid, being the smallest among these matroids in terms of number of circuit-hyperplanes, can be derived from any one of them by a finite number of circuit-hyperplane relaxations. This is similar to the family of non-Ingleton-compliant matroids on 8 points where the Vámos matroid can be obtained from any one of them by circuit-hyperplane relaxations (see [87, Fig. 2]).

Our computational method for finding TTT matroids is as follows.

1. We pick a matroid $\mathcal{M}$ from the matroids database [99] and we define the set H as the set of all circuit-hyperplanes of $\mathcal{M}$.
2. We say that $\mathcal{M}$ is a *TTT* matroid, if at least one subset $A \in \binom{H}{8}$ can be partitioned into $A = A_1 \cup A_2$ with $|A_i| = 4$ satisfying the following properties:
   (a) For every $c \in A_1$, $|\{c' \in A : |c \cap c'| = 3\}| = 4$.

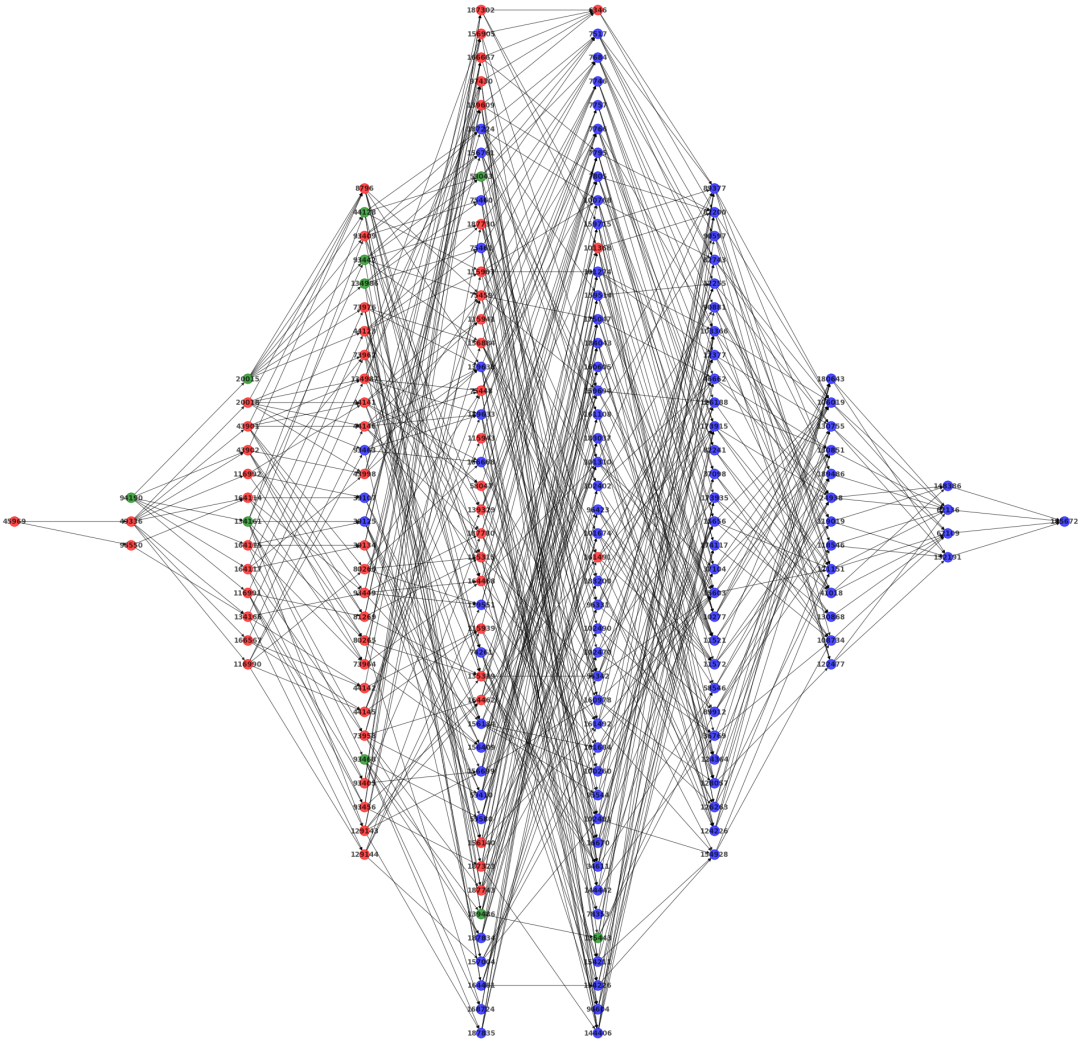


FIGURE 4.3: All TTT matroids on 9 points

(b) For every $c \in A_2$, $|\{c' \in A : |c \cap c'| = 3\}| = 3$.

(c) For every $c \in A_1$, $|\{c' \in A : |c \cap c'| = 2\}| = 3$.

(d) For every $c \in A_2$, $|\{c' \in A : |c \cap c'| = 2\}| = 4$.

(e) $I = \{c \cap c' : c, c' \in A, |c \cap c'| = 3\}$ satisfies $|I| = 6$.

(f) There exist $r, \ell \in I$ such that $r\ell$ is a basis, and they are only contained in two elements of A each.

Fig. 4.3 is arranged from left to right in a descending order by number of circuit-hyperplanes, with the highest being 17 and the lowest being 8. The red nodes are those that have been determined to be non 2-algebraic due to their not being Frobenius-flock representable [28], green ones are not almost entropic due to Vámos and hence not algebraic, while the blue ones have their algebraic status to be undetermined. The labels displayed in the graph are the Bollen ids [27] of these matroids. (For a better viewing of this graph, the interested reader is invited to check the link at `https://github.com/bmilosh/TTT-And-Other-NonRepresentable-Matroids`.)

4.3.2 Duals of TTT Matroids

We know that the dual of a non-Ingleton compliant matroid is also non-Ingleton-compliant [32]. But no such result is known for CI and AK. Indeed, we computationally checked that the duals of most of the TTT matroids are 1-CI (the dual of TTT matroids that are Ingleton-compliant). Next, we show that the duals of all TTT matroids are not 3-CI. Hence, we still do not know any CI-compliant matroid whose dual is not CI-compliant. For AK-compliance, we do not have an analogous example either.

Proposition 4.13. *Duals of TTT matroids are not algebraic and are not 3-CI.*

Proof. The proof that the duals of TTT matroids are not algebraic is direct from the proof that the dual of the Tic-Tac-Toe is not algebraic [60, Proposition 5] and the fact that the classes of sparse-paving matroids and algebraic matroids are minor closed. Hochstättler [60] showed that if the dual of Tic-Tac-Toe were algebraic, it would admit an extension that is also an extension of the Vámos matroid, reaching a contradiction.

In order to prove that duals of TTT matroids are not 3-CI, we follow the ideas of that proof. Let $\mathcal{M}$ be a TTT matroid, with the sets mentioned in Def. 4.8. Let $Q' = r_1r_2r_3$. Now consider the matroid $\mathcal{N} := \mathcal{M}/C\big|(Q')$, i.e., $\mathcal{N}$ is the matroid obtained by contracting C from $\mathcal{M}$ and then restricting to the set Q'. Observe that $\mathcal{N}$ is a rank-5 matroid on 9 points and that the sets r_il_j for $i,j \in \{1,2,3\}$ are circuit-hyperplanes except r_2l_2. For simplicity, let $r_1 = a_1a_2a_3$, $r_2 = b_1b_2b_3$, $r_3 = c_1c_2c_3$ and $l_i = a_ib_ic_i$ for $i \in \{1,2,3\}$.

Consider the dual $\mathcal{N}^*$ of $\mathcal{N}$. Clearly, $\mathcal{N}^*$ is a minor of $\mathcal{M}^*$, and each of $a_1b_1a_2b_2$, $a_1b_1a_3b_3$, $a_2b_2a_3b_3$, $b_1c_1b_2c_2$, $b_1c_1b_3c_3$, $b_2c_2b_3c_3$, $a_1c_1a_2c_2$ and $a_2c_2a_3c_3$ is a rank-3 circuit-hyperplane of $\mathcal{N}^*$.

Now, for the sake of contradition, suppose that $\mathcal{M}^*$ is 3-CI. Then by Lemma 3.15 $\mathcal{N}^*$ is also 3-CI. Let $Q_1 = Q\alpha$ and $Q_2 = Q_1\beta$, and let $\mathcal{N}_1^* = (Q_1, f)$ and $\mathcal{N}_2^* = (Q_2, f)$ be extensions of $\mathcal{N}^*$ where

$$\alpha = CI(a_1b_1, a_2b_2) \text{ and } \beta = CI(b_1c_1, b_2c_2).$$

Since $f(\alpha|a_1b_1a_3b_3) = f(\alpha|a_2b_2a_3b_3) = 0$ and $(a_1b_1a_3b_3, a_2b_2a_3b_3)$ is a modular pair, we have that $f(\alpha|a_3b_3) = 0$ by Lemma 4.10. Analogously, $f(\beta|b_3c_3) = 0$.

The rest of the proof is dedicated to show that $\mathcal{N}_2^*$ is not Ingleton-compliant. We divide it into the following steps, stated as Claims.

Claim 1. $f(a_ic_i\alpha\beta) = 3$ for $i = 1,2,3$.

Suppose, for the sake of contradiction, that $f(a_1\alpha) < 2$. In this case, $f(a_1|\alpha) < 1$ and

$$f(a_1a_2b_2) = f(a_1\alpha a_2b_2) = f(a_1|\alpha a_2b_2) + f(\alpha a_2b_2) \leq f(a_1|\alpha) + 2 < 3,$$

a contradiction. Hence $f(a_1\alpha) = 2$. Next, since

$$1 = f(c_1) \geq f(c_1|a_1\alpha) \geq f(c_1|a_1b_1\alpha) = f(c_1|a_1b_1) = 1$$

we have $f(a_1c_1\alpha) = 1 + f(a_1\alpha) = 3$. Hence $f(a_1b_1c_1\alpha) = f(a_1c_1\alpha) = 3$. Analogously, we can prove that

$$f(a_ic_i\beta) = f(a_ic_i\alpha) = 3 \quad \text{for } i = 1,2,3.$$

Therefore, $3 \leq f(a_i c_i \alpha\beta) \leq f(a_i b_i c_i \alpha\beta) = 3$ for $i = 1, 2, 3$, proving Claim 1.

Now define $A_1 = a_1 c_1$, $A_2 = a_2 c_2$, $A_3 = \alpha\beta$, $A_4 = a_3 c_3$.

Claim 2. $f(A_i A_j A_k) = 4$ for different i, j, k.

Suppose that $f(A_1 A_2 A_3) < 4$. Since $f(a_1 b_1 c_1 \alpha) = f(a_1 c_1 \alpha) = 3$, it implies that $f(A_1 A_2 A_3 b_1) < 4$, a contradiction, because $f(a_1 b_1 c_1 a_2 c_2) = 4$. Analogously, we can prove that $f(A_2 A_3 A_4) = 4$. We know that $f(A_1 A_3 A_4) = f(A_1 A_2 A_4) = 4$ because $A_1 A_4$ is a basis of $\mathcal{N}^*$.

Claim 3. $f(A_3) > 1$.

Suppose that $f(\alpha\beta) = 1$. It implies that $f(\beta|\alpha a_1 b_1) = 0$. Since $f(\beta|b_1 c_1) = 0$ and $\alpha a_1 b_1$ and $b_1 c_1$ are a modular pair, $f(\beta|b_1) = 0$ by Lemma 4.10. Since $f(\beta) = 1$, we also have that $f(b_1|\beta) = 0$. Hence, $2 = f(b_2 c_2) = f(b_2 c_2 \beta) = f(b_1|\beta) + f(b_2 c_2 \beta) \geq f(b_1 b_2 c_2 \beta) = 3$, a contradiction. It proves Claim 3.

According to Claim 1, $f(A_1 A_4) = 4$ and $f(A_i A_j) = 3$ for $(i, j) \neq (1, 4)$. Combining it with Claims 2 and 3 we have that $\mathcal{N}_2^*$ is not Ingleton-compliant and therefore not $1 - CI$, a contradiction. □

From Lemma 4.13, we see that the dual of a TTT matroid is not a folded-linear matroid. It is also a consequence of the fact that TTT matroids are not CI-compliant.

Proposition 4.14. *The duals of TTT matroids are not almost entropic.*

Proof. We checked computationally that the duals of TTT matroids on 9 points are not 3-AK-compliant. The result holds because the family of almost entropic matroids is minor-closed [83]. □

In 1997, it was observed in [60] that, at that time, the Tic-Tac-Toe matroid had all known combinatorial properties of algebraic matroids. Results on algebraic matroids found in the last twenty years are still not enough to check if it is algebraic. One of the motivations of studying this matroid is because it is known that its dual is not algebraic.

4.4 Connections Between Matroid Intersection Properties

Here, we show how the intersection properties mentioned in Section 2.3.2 are connected with other matroid properties like the Ingleton inequality and the common information property.

Following Section 2.3.2, we define $\mathcal{M}_{CI}$ as the class of CI-compliant matroids. As we saw in Section 4.2, $\mathcal{M}_{lin} \subsetneq \mathcal{M}_{CI}$, i.e., there are non-linear matroids that are CI-compliant. In the rest of this section, we analyze the connection between $\mathcal{M}_{CI}$ and $\mathcal{M}_{LP}$, $\mathcal{M}_{GP}$, and $\mathcal{M}_{EP}$. We start with the following result which establishes the position of the common information property with respect to these intersection properties in the case of rank-4 matroids.

Theorem 4.15. *Let $\mathcal{M}^4_{LP}, \mathcal{M}^4_{GP}, \mathcal{M}^4_{EP}$ and $\mathcal{M}^4_{lin}$ be as described in Section 2.3.2. Also let $\mathcal{M}^4_{CI}$ be the class of all CI-compliant rank-4 matroids. Then*

$$\mathcal{M}^4_{lin} \subsetneq \mathcal{M}^4_{CI} \subsetneq \mathcal{M}^4_{LP} = \mathcal{M}^4_{GP} = \mathcal{M}^4_{EP}.$$

Proof. Theorem 2.25 shows that non-LP rank-4 matroids do not satisfy the bundle condition. We also know that rank-4 matroids not satisfying the bundle condition are not CI-compliant (see Section 3.4). Hence, we can conclude that $\mathcal{M}^4_{CI} \subseteq \mathcal{M}^4_{LP}$. Since the dual of the Tic-Tac-Toe matroid is a rank-4 matroid that satisfies the bundle condition and is not CI-compliant, we have that this inclusion is strict.

Taking into consideration that there exist CI-compliant rank-4 matroids that are not linearly representable, for example, the L'_8 and P_3 matroids (Theorem 4.1), we have that $\mathcal{M}^4_{lin} \subsetneq \mathcal{M}^4_{CI}$. The rest of the inclusions are due to Proposition 2.23. □

The problem arising when comparing $\mathcal{M}_{CI}$ to other classes of matroids is that the *CI*-extensions of matroids are polymatroids, in general. Perhaps it would be worth exploring the notion of *CIM-matroids*, defined below.

Definition 4.16. Let $\mathcal{M} = (Q, r)$ be a matroid. We say that $\mathcal{M}$ is a *1-CIM-compliant* matroid if for every pair of subsets $A_0, A_1 \subseteq Q$ there exists a matroid extension (QQ_0, r) of $\mathcal{M}$ such that Q_0 is the common information of the pair (A_0, A_1). Analogously, we can define k-CIM-compliance and CIM-compliance.

Proposition 4.17. *Let $\mathcal{M}_{CIM}$ be the family of CIM matroids. The following inclusions hold:*

$$\mathcal{M}_{CIM} \subseteq \mathcal{M}_{CI} \text{ and } \mathcal{M}_{1-CIM} \subseteq \mathcal{M}_{GP}.$$

Proof. The first inclusion holds because from any matroid $\mathcal{M} = (QQ_0, r)$ we can define a polymatroid $\mathcal{S} = (Qx_0, r')$ with $r'(A) = r(A)$ and $r'(Ax_0) = r(AQ_0)$ for every $A \subseteq Q$.

Let $A_0, A_1 \subseteq Q$ be a non-modular pair. If the matroid is 1-CIM compliant, there exists a matroid extension $\mathcal{M}' = (QQ_0, r)$ of $\mathcal{M}$ such that Q_0 is the common information of the pair (A_0, A_1). Then any $p \in Q_0$ lies in the closure of A_0 and in the closure of A_1 in $\mathcal{M}'$, and the matroid $\mathcal{M}' \setminus (Q_0 - p)$ is an extension of $\mathcal{M}$ on Qp. □

Notice that we do not know if 1-CI implies the generalized Euclidean property, because when we add a common information to a matroid we can obtain a polymatroid that is not a matroid, in general.

Recalling Proposition 3.8, we give a definition of what we call the generalized bundle condition.

Definition 4.18. We say a sparse-paving matroid on $n \geq 8$ points with rank $k \geq 4$ satisfies the *generalized bundle condition* if for any five pairwise disjoint subsets B, A_1, A_2, A_3, A_4 of the ground set with $|B| = k - 4$ and $|A_i| = 2$, the following holds: if five of the six sets of the form BA_iA_j with $i \neq j$ are circuit-hyperplanes, then all six sets are circuit-hyperplanes.

Just like the bundle condition for rank-4 matroids, we show below that matroids that do not satisfy the generalized bundle condition also do not satisfy these 3 intersection properties. However, we make no such claims about the converse statement.

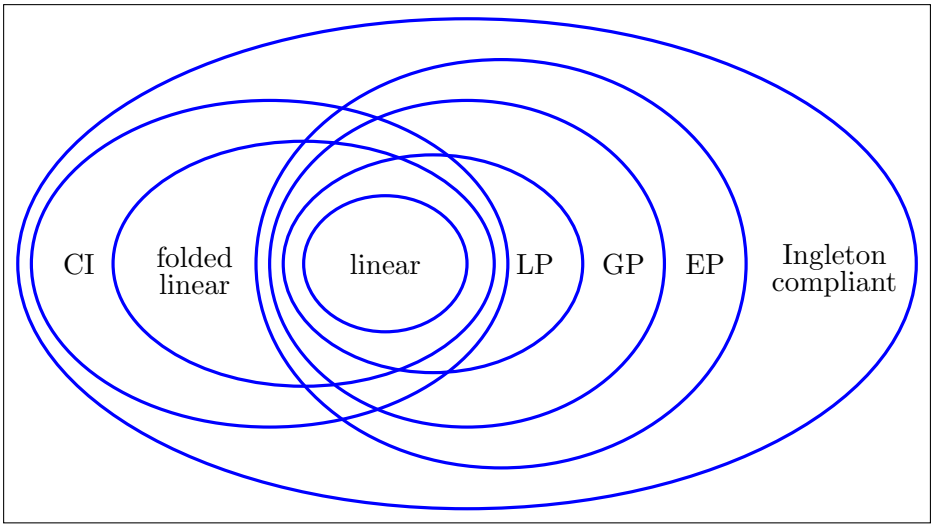


FIGURE 4.4: Intersection Properties and Sparse-Paving Matroids.

Proposition 4.19. *Sparse-paving EP matroids satisfy the generalized bundle condition.*

Proof. Let $\mathcal{M} = (Q, r)$ be a sparse-paving matroid not satisfying the generalized bundle condition. Then $\mathcal{M}$ has the sets mentioned in Def. 4.18. Without loss of generality, assume that BA_3A_4 is a basis. Suppose, for the sake of contradiction, that $\mathcal{M}$ is EP. Then there exists a proper one-element extension $\mathcal{M}'$ on Qp in which p lies in the closures of the hyperplane BA_1A_3 and the line A_4.

Let M be the modular cut on $\mathcal{M}$ defined by this extension. M contains BA_1A_3 and A_4, and, by monotonicity, BA_1A_4 and BA_2A_4 are also in M. Since BA_1A_4 and BA_1A_3 form a modular pair, $BA_1 \in M$. This then implies that $BA_1A_2 \in M$ by monotonicity, and $BA_2 \in M$ by modularity of BA_1A_2 and BA_2A_4. Monotonocity then implies $BA_2A_3 \in M$, and modularity of BA_2A_3 and BA_1A_3 implies $BA_3 \in M$. Finally, modularity of A_4 and BA_3 implies $\emptyset \in M$, which is a contradiction. □

Alfter and Hochstättler [3] proved that the Tic-Tac-Toe matroid does not satisfy the GP property, and an exhaustive search on $(5, 9)$ matroids showed the following result.

Proposition 4.20. *TTT matroids are the only Ingleton-compliant sparse-paving* $(5, 9)$ *matroids that are not GP.*

Clearly, TTT matroids also do not satisfy LP. On the other hand, a computational check showed that they, along with all other Ingleton-compliant $(5, 9)$ matroids, satisfy EP.

Remark 4.21. The connections in Figure 4.4 can be seen as follows. Combining Proposition 4.19 with Proposition 2.22 and the result of Nelson and van der Pol [90], we have that the family of Ingleton-compliant sparse-paving matroids also contains sparse-paving matroids that satisfy any of the 3 intersection properties.

Also, every folded-linear matroid is CI-compliant, and every CI-compliant matroid is Ingleton-compliant (see Section 3.4). However, the relationship between folded-linear matroids and these intersection properties has not been studied as far as we know,

and we do not study it here either. TTT matroids are Ingleton-compliant but not CI-compliant nor GP. We still do not have any proven AK-compliant sparse-paving matroid that is not CI-compliant.

As originally designed, the intersection properties discussed in this section only deal with single-element extensions of a matroid, i.e., they do not concern themselves with whether or not a proper point extension itself admits a proper point extension with respect to a given collection of flats. However, we saw that in the same way we extended 1-CI-compliance to k-CI compliance and CI-compliance in full, we could also do the same to these intersection properties. For starters, we define the notion of 1-EP as follows:

Definition 4.22. A matroid $\mathcal{M}$ is 1-EP if for every non-intersecting pair of hyperplane H and line ℓ, there is a proper point extension $\mathcal{M}'$ of $\mathcal{M}$ by an element p such that p lies in the intersection of the $\mathcal{M}'$ closures of H and ℓ.

With this, we can define the notion of k-EP.

Definition 4.23. A matroid $\mathcal{M}$ is said to be k-EP for an integer $k > 1$ if for every non-intersecting pair of hyperplane H and line ℓ, there is a proper point extension $\mathcal{M}'$ of $\mathcal{M}$ by an element p such that p lies in the intersection of the $\mathcal{M}'$ closures of H and ℓ, and $\mathcal{M}'$ is $k-1$-EP.

The definitions of k-GP and k-LP follow analogously.

Our computational method for checking 1-EP can be seen from the definition as follows:

1. We pick a matroid $\mathcal{M}$ from the matroid database [99] and set $\mathcal{F}$ to be the set of all hyperplanes and lines of $\mathcal{M}$.
2. We say $\mathcal{M}$ is non-1-EP if there is a pair of hyperplane H and line ℓ such that:
   (a) $r(H) + r(\ell) > r(H\ell) + r(H \cap \ell)$, i.e., they are a non-modular pair.
   (b) $\mathrm{cl}(\emptyset) \in M_{H,\ell}$ where $\mathrm{cl}(\emptyset)$ is a maximal set of rank 0 and $M_{H,\ell}$ is the modular cut generated by the pair (H, ℓ).

We do the same for finding non-1-GP matroids by substituting the appropriate flats. The interested reader who would like to see what our programs look like (e.g., to see how we employ these recursive definitions) or even improve them is encouraged to check the links mentioned in Section 1.7.

These extended properties have not been studied in previous works, and so the idea here was to see if, perhaps like the CI technique or the Ingleton-Main/Dress-Lovasz checks of [28], we could find some matroids that satisfy these intersection properties at depth 1 but fail at larger depths.

First, we analyzed the five non-linear Ingleton-compliant 8-point matroids referred to in Section 4.2.2. We found that it can also be proved that three of these matroids are not linear by means of EP: P_1 is not 3-EP, while P_2' and P_2'' are both non-4-EP matroids. The other two matroids L_8 and P_3 are 3-EP. These two matroids are not linear but

are folded-linear (Theorem 4.1). As of now, we are not able to distinguish linear from folded-linear matroids by only analyzing intersection properties.

After the analysis described in the previous remark, there are some questions that remain open. Levi's intersection property and the generalized Euclidean intersection are equivalent for rank 4 matroids. We do not know if this equivalence can be extended to sparse-paving matroids or to rank-5 matroids. Also, we know that TTT matroids of rank 5 are not GP. We wonder if there are other non-1-GP Ingleton-compliant sparse-paving rank-5 matroids that are not TTT.

4.5 Other Non-Representable $(5,9)$ Matroids

In this section, we study two other families of $(5,9)$ matroids that are non-linearly representable.

4.5.1 Non Sparse-Paving Matroids

Our main objective in analyzing $(5,9)$ matroids was to find non-CI matroids that were Ingleton-compliant, in order to discover new properties of linear matroids. Checking CI-compliance of matroids on 9 points is computationally expensive, and we could not complete this characterization. Besides TTT matroids, until now we didn't find other Ingleton-compliant sparse-paving $(5,9)$ matroids that are not 1-CI-compliant.

One of the interesting results from [87] is that a 9-point matroid is non-Ingleton-compliant if and only if it has a non-Ingleton-compliant minor. With this, one is able to easier identify the non-Ingleton-compliant matroids on 9 points by checking if it has any of the 39 non-Ingleton-compliant $(4,8)$ matroids as a minor. This is sometimes more efficient than applying the Ingleton inequality itself to see if the matroid is Ingleton-compliant.

In order to find non-CI-compliant *candidate* matroids, we checked the generalized Euclidean intersection property, which is much more efficient. As discussed in Section 4.4, matroids of rank 4 that are CI-compliant are also GP, but we do not know what is the connection between these two properties for matroids of rank 5. Therefore, we made this search considering the option that some non-GP matroids would not be CI-compliant. And indeed, we found some Ingleton-compliant $(5,9)$ matroids other than the TTT matroids that are not 1-GP. They are non sparse-paving matroids and are listed in Table 4.1. Like the TTT matroids, these matroids are 1-EP. Checking further, we saw that these matroids are also not 1-CI. Hence, they are not folded-linear matroids. TTT matroids and these new matroids are the only non-1-GP Ingleton-compliant $(5,9)$ matroids. Therefore, all $(5,9)$ matroids that do not satisfy the generalized Euclidean intersection property at depth 1 are also non-1-CI matroids.

An example is the matroid 201827 with circuit-closures 0125, 0268, and 1568 of rank 3, and circuit-hyperplanes 12378, 03458, 24578, 01467, 12346, and 34678. Observe that the circuits 0125, 0268 and 1568 form a configuration that is present in the Vámos matroid. With the modular cut corresponding to the non-modular pair $(035, 146)$, one is not able to get a proper point extension of the matroid. Hence, it does not satisfy the generalized

199136	204630	211985	221647	227977	233153
199230	204769	216857	221650	228317	233156
199553	204896	217478	221722	228452	233245
199807	204903	217597	221834	229354	233261
200470	204973	217772	221905	229356	241344
200589	205074	217846	221910	229357	241614
200633	205111	218082	222035	229741	243049
200972	206383	218124	222041	229892	243792
201001	206385	218129	222044	230229	243800
201056	206515	218179	222384	230558	243801
201121	206844	218341	222385	231565	244422
201124	206959	220346	222436	231566	244449
201827	206992	220524	223015	231587	245708
201869	207536	220657	223016	231588	245732
201957	207550	221002	223035	231997	245765
201958	207669	221046	223221	232065	253254
202832	208093	221323	223417	232651	253828
204059	211135	221541	227084	232654	
204585	211841	221542	227086	232824	
204624	211983	221635	227789	233072	

TABLE 4.1: Ingleton-Compliant Non Sparse-Paving $(5, 9)$ Non-GP Matroids

Euclidean intersection property. Using this same pair, we found that the matroid is not CI-compliant.

We note that this approach fails for matroids of rank 4 in general as the only rank-4 matroids that do not satisfy the generalized Euclidean intersection property at depth 1 are precisely the ones that have one of the 39 non-Ingleton-compliant $(4, 8)$ matroids as a minor, or in other words, the ones that are not Ingleton-compliant. This is due to two things. The first is that a rank-4 matroid satisfies GP at depth 1 if and only if it satisfies the bundle condition [8]. The second is the observation by Alfter and Hochstättler [3] that "the minimal configuration that violates the bundle condition is the Vámos matroid." Each of the 39 non-Ingleton-compliant (4,8) matroids contains the Vámos configuration and therefore does not satisfy the bundle condition. Hence, if a rank-4 matroid has any of these as a minor, it will not satisfy the bundle condition, and is therefore not a GP matroid.

Checking the duals of the matroids in this family, we found that they break AK at depth 3 and are therefore neither almost entropic nor algebraic.

Proposition 4.24. *The matroids listed in Table 4.1 are Ingleton-compliant and non-1-CI, and their duals are neither 3-CI nor 3-AK.*

4.5.2 Some 1-GP but Non-2-GP Matroids

We analyze a third family of non-linearly representable matroids we found in this section. As we will see in Section 4.6, there are 12,129 $(5, 9)$ matroids with undetermined 2-algebraicity [28]. We investigated these matroids using the intersection properties discussed in Sections 2.3.2 and 4.4. We found that among these matroids, there are some

that are 1-GP but neither 2-GP nor 2-EP. This means they are not linearly representable. However, it is possible that they are folded linear. To investigate further about whether they are folded-linear matroids, we used the CI technique. Doing this we found some of these matroids to be non folded-linear matroids as they are non-2-CI. For the others, we are not able to say whether they are indeed 2-CI due to time constraints. We note that the duals of all these matroids have been shown to be non-algebraic due to failing Ingleton-Main at different depths [27, 28].

While we could not check all 12,129 matroids for 2-EP, the non-2-EP matroids we found are presented in Table 4.2. We observe that the ids used are their Bollen ids [27] since he was the one that enumerated these 12,129 $(5, 9)$ matroids with undetermined 2-algebraicity. In the column marked *"2-CI"* we write *"False"* to indicate those we have determined to be non-2-CI. For the ones we are yet to determine their 2-CI status, we put a dash. The columns marked "U_1, V_1" and "U_2, V_2" indicate the sets that when used together break CI for the matroid at depth 2. We note that these are not necessarily the only combinations of sets that break CI for these matroids; they are just the ones we found.

Matroid	2-CI	U_1, V_1	U_2, V_2
6182	False	03, 127	36, 087
6184	False	03, 127	36, 087
6206	False	03, 127	36, 087
6207	False	03, 127	36, 087
7330	—	—	—
7339	—	—	—
7493	False	03, 127	36, 087
7848	False	57, 280	05, 184
7849	False	57, 280	05, 184
7928	—	—	—
8080	False	03, 128	36, 087
8088	False	46, 018	40, 513
8369	False	03, 127	36, 087
10631	False	03, 128	36, 087
12375	—	—	—
12529	—	—	—
15107	False	03, 128	36, 087
15108	False	03, 128	36, 087
15115	False	03, 128	36, 087
15128	False	03, 128	36, 087
15129	False	03, 128	36, 087
15130	False	03, 128	36, 087
15140	False	03, 128	36, 087
15177	False	03, 128	36, 087
15183	False	03, 128	36, 087
15189	False	03, 128	36, 087
15387	—	—	—
18212	False	46, 018	04, 135
26185	False	03, 128	36, 087
26186	False	03, 128	36, 087
26224	False	03, 128	36, 087

Table 4.2 continued from previous page

Matroid	2-CI	U_1, V_1	U_2, V_2
26227	False	03, 128	36, 087
26584	False	46, 018	40, 513
37250	False	03, 128	36, 087
37253	False	03, 128	36, 087
37255	False	03, 128	36, 078
39113	—	—	—
42465	False	03, 128	36, 087
42484	False	36, 078	03, 128
42525	False	03, 128	36, 087
42526	False	03, 128	36, 087
46632	False	15, 087	01, 237
55425	False	15, 087	01, 237
56908	—	—	—
58384	False	03, 127	36, 087
59382	False	03, 127	36, 087
77860	False	03, 128	36, 087
83155	False	03, 128	36, 087
83156	False	03, 128	36, 087
83600	False	46, 018	40, 513
88940	False	03, 127	36, 087
88967	False	03, 127	36, 087
89019	False	03, 127	36, 087
89044	False	03, 127	36, 087
89045	False	03, 127	36, 087
89046	False	03, 127	36, 087
89392	—	—	—
91265	False	03, 128	36, 087
95347	—	—	—
95369	—	—	—
95441	False	03, 127	36, 087
95446	False	03, 127	36, 087
96490	False	03, 128	36, 087
96491	False	46, 018	40, 513
100320	False	03, 128	36, 087
100321	False	03, 128	36, 087
100325	False	03, 128	36, 087
100333	—	—	—
100676	—	—	—
100735	False	03, 127	36, 087
100736	False	03, 127	36, 078
100755	False	03, 127	36, 087
100947	False	03, 127	36, 087
100983	False	03, 127	36, 087
100988	False	03, 127	36, 087
101262	—	—	—
101455	—	—	—
103147	False	03, 127	36, 087

Table 4.2 continued from previous page

Matroid	2-CI	U_1, V_1	U_2, V_2
104169	False	03, 128	36, 087
106805	False	03, 128	36, 087
111823	False	03, 128	36, 087
111839	False	03, 128	36, 087
111871	False	03, 128	36, 087
127707	False	03, 128	36, 087
127710	False	03, 128	36, 087
127720	False	03, 128	36, 087
127742	False	03, 128	36, 087
127743	False	03, 128	36, 087
135432	False	03, 127	36, 087
136699	False	03, 127	36, 087
139606	—	—	—
139632	—	—	—
139657	—	—	—
140204	False	03, 127	36, 087
144432	False	57, 280	05, 184
145710	False	03, 127	36, 087
146335	False	15, 087	01, 237
146367	False	03, 127	36, 087
146368	False	03, 127	36, 087
146556	—	—	—
146946	False	03, 128	36, 087
147269	False	03, 127	36, 087
154115	False	03, 127	36, 087
156003	—	—	—
156059	False	03, 127	36, 087
156062	False	03, 127	36, 087
156063	—	—	—
156183	False	04, 218	20, 613
156366	False	03, 127	36, 087
156413	—	—	—
156972	—	—	—
158280	False	03, 128	36, 087
158723	—	—	—
159112	False	03, 127	36, 087
159119	False	03, 127	36, 087
159177	—	—	—
159184	False	03, 127	36, 087
159185	False	03, 127	36, 087
159202	False	03, 127	36, 087
159236	False	03, 127	36, 087
159241	False	03, 127	36, 087
159242	False	03, 127	36, 087
159245	False	03, 127	36, 087
159246	False	03, 127	36, 087
159288	—	—	—

Table 4.2 continued from previous page

Matroid	2-CI	U_1, V_1	U_2, V_2
161127	—	—	—
164382	False	03, 127	36, 087
171854	—	—	—
171945	False	03, 127	36, 087
171946	False	03, 127	36, 087
171954	False	03, 127	36, 087
171967	False	03, 127	36, 087
172039	False	03, 127	36, 087
172042	False	03, 127	36, 087
174258	False	03, 128	36, 087
180080	—	—	—
183134	—	—	—
183655	—	—	—
183825	—	—	—
183860	False	03, 128	36, 087
183866	False	03, 128	36, 087
183877	False	03, 128	36, 087
184061	False	46, 018	40, 513
187245	False	03, 127	36, 087
187929	False	03, 127	36, 087
190074	False	03, 128	36, 087
190075	False	03, 128	36, 087

TABLE 4.2: Some 1-GP but Non-2-GP $(5, 9)$ Matroids

4.6 Matroids, Flocks, and Algebraicity

Bollen in his thesis [28] found new and interesting results on the algebraicity of certain matroids over fields of characteristic 2 (such matroids are called 2-algebraic) using Frobenius flocks and other tools. In this section we analyze his results and combine them with ours to have a clearer picture of the algebraic and almost entropic status of matroids on up to 9 points as they are today.

We refer the reader to [28] for a very detailed discussion on Frobenius-flock representability. An important result of his work is the following theorem.

Theorem 4.25. *[28, Thm. 5.1] Let K be an algebraically closed field of nonzero characteristic. Then every algebraic matroid over K is Frobenius-flock representable over K.*

Using this tool and other necessary conditions for a matroid to be algebraic, like the Ingleton-Main Lemma [62] and also the Dress-Lovasz condition [46], he solved the question of algebraicity in characteristic 2 of many matroids on up to 9 points. We discuss his results below.

2-Algebraic	$(4, 8)$	$(3, 9)$	$(4, 9)$	$(5, 9)$	$(6, 9)$
True	897	1,271	148,822	148,822	1,271

False	40	1	31,820	29,263	1
Unknown	3	3	9,572	12,129	3

TABLE 4.3: 2-Algebraic matroids on 8 and 9 elements [28]

(r, n)	$(4, 8)$	$(4, 9)$	$(5, 9)$
DL	39	27,137	27,137
DL depth 2	39	27,137	27,137
IM depth 3	39	28,418	27,144
IM depth 4	39	30,171	27,442
IM depth 5	39	30,658	27,500

TABLE 4.4: Dress-Lovasz (DL) and Ingleton-Main (IM) check [28]

1. He found no new results on algebraicity for:
   (a) (r, n) matroids for $r \leq n \leq 8$.
      i. The 39 $(4, 8)$ matroids he found to be non-algebraic due to Ingleton-Main are just the Vámos matroid and the other 38 with the Vámos configuration. The other matroid not 2-algebraic is linear over fields of characteristic 3 and is therefore algebraic.
      ii. The algebraicity of P_1, P_2' and P_2'' remains unknown.
   (b) $(3, 9)$ and $(6, 9)$ matroids.
      i. There are 3 $(3, 9)$ matroids for which algebraicity is unknown. These matroids are obtained from the non-Pappus matroid by circuit-hyperplane 'derelaxations'. Their $(6, 9)$ duals also have algebraicity as an open question.
2. For $(4, 9)$ matroids, he found that:
   (a) There are 4,551 $(4, 9)$ matroids that are not 2-algebraic due to their not being Frobenius-flock representable. Of these, 1,064 satisfied other conditions for algebraicity (e.g., Dress-Lovasz and Ingleton-Main conditions) except Frobenius-flock representability.
   (b) There are 317 $(4, 9)$ matroids for which Frobenius-flock representability is unknown. However, these matroids are all non-algebraic due to Dress-Lovasz.
   (c) In general, there are 9,572 $(4, 9)$ matroids whose 2-algebraicity is unknown.
3. For $(5, 9)$ matroids, he found that:
   (a) There are 4,551 $(5, 9)$ matroids that are not 2-algebraic due to their not being Frobenius-flock representable. Of these, 1,763 satisfied other conditions for algebraicity (e.g., Dress-Lovasz and Ingleton-Main conditions) except Frobenius-flock representability.
   (b) There are 315 $(5, 9)$ matroids for which Frobenius-flock representability is unknown. However, these matroids are all non-algebraic due to Dress-Lovasz.
   (c) In general, there are 12,129 $(5, 9)$ matroids whose 2-algebraicity is unknown.

4. The 27,137 $(4, 9)$ matroids that break Dress-Lovasz at depth 1 are precisely the $(4, 9)$ matroids with the Vámos configuration. Same applies to their duals.

In addition to these, he also found 14 matroids that he called "Tic-Tac-Toe matroid and its siblings." It is not entirely clear what he means by this, although he does describe the Tic-Tac-Toe matroid as "a matroid which is closed under Dress-Lovasz extensions, but whose dual is non-algebraic due to the Dress-Lovasz condition at depth 3," and goes on to say "we found that there are 14 $(5, 9)$ matroids with this property," but we assume that he is in fact referring to some of the 181 $(5, 9)$ matroids we found having the TTT configuration. He found that though these 14 matroids are Frobenius-flock representable, their algebraicity remains open.

However, we should note that he was indeed able to find that 62 of the TTT matroids are not Frobenius-flock representable in characteristic 2. And here we see the second break in uniform behaviour among TTT matroids, the first being that some of them are non-Ingleton-compliant since they have a Vámos minor.

While Bollen's results are on algebraicity, we can combine parts of it with ours to observe the following about the almost entropicity of (r, n) matroids for $r \leq n \leq 9$.

Remark 4.26. There are at least 39 $(4, 8)$ matroids that are not almost entropic and 3 for which almost entropicity is unknown. All others are almost entropic.

Remark 4.27. There are at least 27,425 and 27,137 $(4, 9)$ and $(5, 9)$ matroids, respectively, that are not almost entropic. The difference of 288 represents the duals (all non 3-AK) of the Ingleton-compliant TTT matroids and the matroids in Section 4.5.1 while the common figure of 27,137 represents the non-AK matroids with the Vámos configuration.

Chapter 5

Secret Sharing for Matroid Ports

5.1 Introduction

Like in the previous chapter, we present here some of the results from [10] that pertain to secret sharing.

We start off with some definitions that were not covered in Chapter 2. In Section 5.3, we discuss the LP technique applied to the search for lower bounds on the information ratio of secret sharing schemes. In particular, we show the improvements presented in [50] where the CI and AK properties were used to obtain better bounds on the information ratio of secret sharing schemes for different families of access structures.

We show in Section 5.3.1 that the same technique can be applied in network coding to obtain bounds on the coding capacities of networks. The CI property can be used to obtain upper bounds on the linear coding capacity while the AK property can be applied in the general case. Taking the Vámos network, which has a linear coding capacity of 5/6 [42], we showed that the 10/11 upper bound on its coding capacity in the general case can also be obtained using the AK property.

Our focus for secret sharing was on matroid ports. Farràs et al. [50] found bounds on the information ratio of secret sharing schemes for ports of some 8-point matroids. We extend this result by considering all matroids on 8 points. The linear ones all satisfy the CI property, and hence, have the trivial bound on λ. However, we found non-trivial bounds on both λ and σ for the ports of all 39 non-Ingleton-compliant 8-point matroids. This gives a separation result that applies to all sparse-paving non-Ingleton-compliant matroids: ports of such matroids have lower bounds of at least 4/3 on λ and 9/8 on σ. We also have that the current best lower on the information ratio of secret sharing schemes for matroid ports is the 8/7 bound on σ held by some of the ports of the F_8 matroid.

Moving further, we also looked at ports of 9-point matroids. First, we studied some non-Ingleton-compliant matroids on 9 points and found bounds consistent with the separation result for such matroids. We also found non-trivial bounds on λ for all the Ingleton-compliant matroids described in Sections 4.3 and 4.5.1. For the Tic-Tac-Toe matroid, we give a construction for the 6/5 bound on λ for one of its ports, thereby showing that the bound is tight (Section 5.4).

In Section 5.5, we present more results on secret sharing, but specifically for the ports of sparse-paving matroids and using different methods than the LP technique. The first result to be highlighted from this section is that ports of sparse-paving matroids are slice access structures [15] of the form $S_{r-1,r+1}$. We also found that ports of sparse-paving matroids admit secret sharing schemes with share size $2^{O(\sqrt{n}\log n)}$ (Theorem 5.9). This result means that current upper bounds that apply to almost all access structures [15] also apply to ports of sparse-paving matroids. Other results in this section make use of counting arguments to give exponential lower bounds on the information ratio and total share size of linear secret sharing schemes—with 1-bit secrets—for ports of sparse-paving matroids as $2^{n/3-o(n)}$ and $2^{n/2-o(n)}$, respectively.

Finally, we note that the reader interested in seeing the constant bounds we obtained for the ports of 8- and 9-point matroids we discussed will find them at Appendix B.

5.2 Preliminaries

Definition 5.1. An *access function* on a finite set P is a map $\Gamma\colon \mathcal{P}(P) \to \mathbb{R}$ satisfying the following properties.

1. $\Gamma(\emptyset) = 0$ and $\Gamma(P) = 1$.
2. $\Gamma(X) \leq \Gamma(Y)$ if $X \subseteq Y \subseteq P$.

An access function is *perfect* if its only values are 0 and 1. The *qualified* and *forbidden* sets of the access function Γ are the ones with $\Gamma(X) = 1$ and, respectively, $\Gamma(X) = 0$.

Definition 5.2. For a polymatroid (Q, f) and a point $p_o \in Q$ with $f(p_o) > 0$ and $f(Q \smallsetminus p_o) = f(Q)$, the *port of the polymatroid* (Q, f) *at* p_o is the access function Γ on the set $P = Q \smallsetminus p_o$ defined by

$$\Gamma(X) = \frac{f(X{:}p_o)}{f(p_o)}.$$

The *dual* Γ^* of an access function Γ on P is defined by $\Gamma(X) = 1 - \Gamma(P \smallsetminus X)$ for every $X \subseteq P$. If Γ is the port of a matroid $\mathcal{M}$ at p_o, then its dual Γ^* is the port of the dual matroid $\mathcal{M}^*$ at p_o. Consider an access function Γ on P and a subset $B \subseteq P$. If $\Gamma(P \smallsetminus B) = 1$, the access function $\Gamma \setminus B$ on $P \smallsetminus B$ defined by $(\Gamma \setminus B)(X) = \Gamma(X)$ is the *deletion of* B *from* Γ. If $\Gamma(B) = 0$, the access function (Γ/B) with $(\Gamma/B)(X) = \Gamma(XB)$ is the *contraction of* B *from* Γ. Every access function that is obtained from Γ by deletions and contractions is a *minor* of Γ. If Γ is the port of a polymatroid $\mathcal{M} = (Q, f)$ at p_o and $B \subseteq P = Q \smallsetminus p_o$, then the minors $\Gamma \setminus B$ and Γ/B are the ports of $\mathcal{M} \setminus B$ and, respectively, $\mathcal{M}/B$ at p_o.

Definition 5.3. Let P be a finite set of *players* and $Q = Pp_o$ with $p_o \notin P$. Let Γ be an access function on P. Let $S = (S_x)_{x\in Q}$ be a discrete random vector and (Q, h) the entropic polymatroid determined by S. Then S is a *secret sharing scheme* on P with access function Γ if the following properties are satisfied.

1. $h(p_o) > 0$ and $h(P) = h(Pp_o)$.

2. Γ is the port of (Q, h) at p_o.

The random variable S_{p_o} corresponds to the *secret value*, and the *share* for a player $x \in P$ is given by the random variable S_x. *Linear* secret sharing schemes are those defined by linear random vectors. A secret sharing scheme is *perfect* if its access function is perfect. The *information ratio* of a secret sharing scheme is $\max_{x \in P} h(x)/h(p_o)$, that is, the ratio between the maximum length of the shares and the length of the secret.

As we mentioned in the Introduction, only perfect secret sharing schemes are considered in this thesis. Perfect access functions are also called *access structures*. Each of them is determined by its minimal qualified sets. An access structure is *connected* if every player is in some minimal qualified set. All access structures in this thesis are supposed to be connected. In a perfect scheme, $h(x) \geq h(p_o)$ for every $x \in P$. A perfect secret sharing scheme is *ideal* if $h(x) = h(p_o)$ for every $x \in P$. The *optimal information ratio* $\sigma(\Gamma)$ of an access structure Γ is the infimum of the information ratios of the secret sharing schemes for Γ, while $\lambda(\Gamma)$ is the corresponding value when restricting the optimization to linear secret sharing schemes.

A matroid is *connected* if every pair of points in the ground set lie in a common circuit. All ports of a connected matroid are connected access structures. Moreover, a connected matroid is determined by any of its ports.

Let $S = (S_x)_{x \in Q}$ be an ideal secret sharing scheme and let h be the entropic vector associated to S. Then the polymatroid (Q, f) defined by $f(X) = h(X)/h(p_o)$ for every $X \subseteq Q$ is a matroid [31]. As a consequence, the access structures of ideal secret sharing schemes coincide with the ports of entropic matroids, and the ports of folded linear matroids are precisely the access structures of ideal linear secret sharing schemes.

5.3 LP Technique Applied to Secret Sharing

We describe next the linear programming technique that has been extensively used (see the references in [50]) to find lower bounds in secret sharing and the improvement on it proposed in [50].

Several new lower bounds on the information ratio of secret sharing schemes have been obtained by using the improved linear programming technique [50]. For instance, by using the common information property, the exact values of the optimal information ratios of *linear* secret sharing schemes for *all* access structures on five players and *all* graph access structures on six players have been determined, concluding the projects undertaken in [65, 108] when restricted to linear schemes. Moreover, some of the existing lower bounds for general (that is, non-linear) secret sharing schemes for those and other access structures have been improved by using the AK-common information. The analogous application of the copy lemma has been described in [58].

On the negative side, the application of that technique is currently limited to solving linear programming problems that provide bounds for particular cases. Moreover, because of the huge number of variables and constraints, only problems with small size can be solved. In contrast, several general results, such as the best known general lower bound for secret sharing [36], have been obtained from the simpler technique involving only Shannon inequalities.

The search for new techniques to derive linear rank and information inequalities and further improve the aforementioned linear programming technique is worth undertaking. For example, the common information property is solely based on the intersection of vector subspaces. It is possible that a deeper use of linear algebra, as in the search for characteristic-dependent linear rank inequalities [45, 94], will provide some results.

Let $(S_x)_{x\in Q}$ be a secret sharing scheme with access structure Γ on the set of players $P = Q\smallsetminus p_o$. Let (Q, h) be the entropic polymatroid determined by it and take the polymatroid (Q, f) given by $f(X) = h(X)/h(p_o)$. Then the vector $(f(X))_{X\in\mathcal{P}(Q)}$ satisfies the linear constraints

(N) $f(p_o) = 1$,

(Γ) $f(X{:}p_o) = \Gamma(X)$ for every $X \subseteq P$

and also the polymatroid axioms (P1)–(P3) in Definition 2.13. Therefore, the vector f is a feasible solution of Linear Programming Problem 5.

Linear Programming Problem 5. For an access structure Γ on the set P, the optimal value of this linear programming problem is, by definition, $\kappa(\Gamma)$.

$$\begin{array}{ll} \text{Minimize} & v \\ \text{subject to} & v \geq f(x) \text{ for every } x \in P \\ & \text{(N)}, (\Gamma), \text{(P1)}, \text{(P2)}, \text{(P3)} \end{array}$$

Since this applies to every secret sharing scheme with access structure Γ and the objective function equals the information ratio, the optimal value $\kappa(\Gamma)$ of this linear programming problem is a lower bound on $\sigma(\Gamma)$. It is the best lower bound that can be obtained by using only Shannon information inequalities [36, 78]. That linear program can be improved by adding non-Shannon information inequalities [18, 89, 93] or, as proposed in [50], constraints derived from AK-information or common information.

Linear Programming Problem 6. Consider an access structure Γ on a set P and a pair (A_0, A_1) of subsets of P. The optimal value of this linear programming problem is a lower bound on $\lambda(\Gamma)$.

$$\begin{array}{ll} \text{Minimize} & v \\ \text{subject to} & v \geq f(x) \text{ for every } x \in P \\ & \text{(N)}, (\Gamma) \\ & \text{(C1)}, \text{(C2)} \text{ for } (A_0, A_1) \text{ and } x_o \\ & \text{(P1)}, \text{(P2)}, \text{(P3)} \text{ on the set } Qx_o. \end{array}$$

Linear Programming Problem 7. Let $U, V, Z \subseteq P$. The optimal value of this linear programming problem is a lower bound on $\sigma(\Gamma)$.

$$\begin{array}{ll} \text{Minimize} & v \\ \text{subject to} & v \geq f(x) \text{ for every } x \in P \\ & (\text{N}), (\Gamma) \\ & (\text{AK1}), (\text{AK2}), (\text{AK3}) \text{ on } z_0 \text{ and } (U, V, Z) \\ & (\text{P1}), (\text{P2}), (\text{P3}) \text{ on the set } Qz_o. \end{array}$$

These linear programming problems can be extended by adding the common information or the AK-information for more pairs or, respectively, triples of sets.

5.3.1 Application of LP Technique to Network Coding

The search for lower bounds on the information ratio in secret sharing is somewhat similar to the search for upper bounds on the coding capacity in network coding. Hence, the linear programming problems just described can also be applied in network coding to find bounds on the coding capacities of different networks. Since there is a linear network coding capacity and a general network coding capacity, we observe that the CI technique can be used to obtain bounds on the linear coding capacity of a network, while the AK technique can be useful in obtaining bounds for the general case.

Dougherty, Freiling and Zeger [42] showed the limitations of using Shannon-type information inequalities in the search for bounds on network coding capacities, which is similar to the case in secret sharing. Using the Zhang-Yeung inequality, they proved a better bound on the coding capacity of the Vámos network (which is derived from the Vámos matroid) than was obtained using Shannon-type information inequalities. In particular, they proved that Shannon-type inequalities can only prove an upper bound of 1, while non-Shannon-type inequalities can prove an upper bound of 10/11. For the linear coding capacity of this network, they showed that it is exactly 5/6.

Applying the AK technique to the Vámos network, we found that we could only get the same 10/11 upper bound on its coding capacity. This shows that these techniques can indeed be applied in the search for bounds in network coding as well.

5.4 Lower Bounds on The Information Ratio for Matroid Ports

Consider a finite set of players P, a special player $p_o \notin P$ and $Q = Pp_o$. For a polymatroid (Q, f), we notate $\Gamma_o(f)$ for its port at p_o and $\sigma(f) = \max_{x \in P} f(x)/f(p_o)$. Let Γ be a connected access structure on the set P. Then the parameters $\sigma(\Gamma)$ and $\lambda(\Gamma)$ introduced in Section 5.2 and the optimal value $\kappa(\Gamma)$ of Linear Programming Problem 5 are characterized as follows.

- $\kappa(\Gamma) = \min\{\sigma(f) : (Q, f) \text{ is a polymatroid with } \Gamma = \Gamma_o(f)\}$.
- $\sigma(\Gamma) = \inf\{\sigma(f) : (Q, f) \text{ is an entropic polymatroid with } \Gamma = \Gamma_o(f)\}$.

- $\lambda(\Gamma) = \inf\{\sigma(f) : (Q, f)$ is a linear polymatroid with $\Gamma = \Gamma_o(f)\}$.

The following parameter has been recently introduced by Csirmaz [37].

- $\overline{\sigma}(\Gamma) = \min\{\sigma(f) : (Q, f)$ is an almost entropic polymatroid with $\Gamma = \Gamma_o(f)\}$.

Clearly, $1 \leq \kappa(\Gamma) \leq \overline{\sigma}(\Gamma) \leq \sigma(\Gamma) \leq \lambda(\Gamma)$. Moreover, Γ is a matroid port if and only if $\kappa(\Gamma) = 1$, and this is equivalent to $\kappa(\Gamma) < 3/2$ [78, Theorem 4.4]. An access structure admits an ideal secret sharing scheme if and only if it is the port of an entropic matroid. Besides, $\overline{\sigma}(\Gamma) = 1$ if and only if Γ is the port of an almost entropic matroid. The parameters κ and λ are invariant by duality, that is, $\kappa(\Gamma^*) = \kappa(\Gamma)$ and $\lambda(\Gamma^*) = \lambda(\Gamma)$ for every access structure Γ. By the recent results in [37, 67], this is not the case for the parameter $\overline{\sigma}$. If the access structure Γ' is a minor of Γ, then $\kappa(\Gamma') \leq \kappa(\Gamma)$, $\lambda(\Gamma') \leq \lambda(\Gamma)$, and also $\overline{\sigma}(\Gamma') \leq \overline{\sigma}(\Gamma)$.

By using the techniques described in Section 5.3, new lower bounds on $\overline{\sigma}(\Gamma)$ and $\lambda(\Gamma)$ were obtained in [50] for several access structures including the ports of the matroids $AG(3,2)'$, F_8, Q_8, and V_8. Moreover, the bounds on $\lambda(\Gamma)$ for the ports of Q_8 and V_8 are tight [50]. Subsequently, an improved lower bound on $\overline{\sigma}(\Gamma)$ for a port of the Vamos matroid V_8 was obtained in [58] by using the copy lemma instead of the Ahlswede–Körner lemma.

In this thesis, we continued the search for lower bounds for matroid ports by using those methods, which, of course, provide relevant lower bounds only when applied to matroids that are not CI-compliant. We began by exploring the ports of the 39 matroids on 8 points that are not Ingleton-compliant and we found out that all of them satisfy $\lambda(\Gamma) \geq 4/3$ and $\overline{\sigma}(\Gamma) \geq 9/8$. A more general result is obtained by combining our bounds with Corollary 3.9.

Theorem 5.4. *If a sparse-paving matroid is not Ingleton-compliant, then at least eight of its ports satisfy* $\lambda(\Gamma) \geq 4/3$ *and* $\overline{\sigma}(\Gamma) \geq 9/8$.

Proof. Let $\mathcal{M} = (Q, r)$ be a sparse-paving matroid that is not Ingleton-compliant. By Corollary 3.9, it has a minor $\mathcal{M}' = (Q', r')$ with $|Q'| = 8$ that is not Ingleton-compliant. Hence $\mathcal{M}'$ is one of the 39 matroids on 8 points that are not Ingleton-compliant. For every $p_o \in Q' \subseteq Q$, the port Γ' of $\mathcal{M}'$ at p_o is a minor of the port Γ of $\mathcal{M}$ at p_o. Therefore, $\lambda(\Gamma) \geq \lambda(\Gamma') \geq 4/3$ and $\overline{\sigma}(\Gamma) \geq \overline{\sigma}(\Gamma') \geq 9/8$. □

Better lower bounds on $\overline{\sigma}(\Gamma)$ have been obtained for some of those 39 matroids and are presented in Table B.1. The names or numbers of the matroids are as they appear in [87], and in the database [99].

We also applied the linear programs in Section 5.3 to the ports of many 9-point matroids, including some that are Ingleton-compliant, like the TTT matroids mentioned in Sec. 4.3. While we were able to find non-trivial lower bounds on $\lambda(\Gamma)$ for a number of these matroids (see Appendix B), we found no non-trivial bounds on $\overline{\sigma}(\Gamma)$ for the Ingleton-compliant matroids we checked.

By presenting a suitable linear secret sharing scheme, we prove next that the bound $\lambda(\Gamma) \geq 6/5$ is tight for at least one of the ports of the Tic-Tac-Toe matroid.

Proposition 5.5. *There is a port* Γ *of the Tic-Tac-Toe matroid with a lower bound* $6/5$ *on* $\lambda(\Gamma)$.

Proof. Take $Q = \{0,1,2\} \times \{0,1,2\}$ and, for every $(a,b) \in Q$, the 5-element set

$$C_{ab} = \{(i,j) \in Q : i = a \text{ or } j = b\}.$$

We introduce several sparse-paving matroids with ground set Q and rank 5. We call $\mathcal{M}_o$ the one whose circuit-hyperplanes are all sets C_{ab}. The *Tic-Tac-Toe matroid* $\mathcal{M}$ is obtained from $\mathcal{M}_o$ by relaxing the circuit C_{11}. Finally, for every $(a,b) \neq (1,1)$, let $\mathcal{M}_{ab}$ be the matroid that is obtained from the Tic-Tac-Toe matroid by relaxing the circuit C_{ab}. Clearly, every matroid $\mathcal{M}_{ab}$ is isomorphic to either $\mathcal{M}_{00}$ or $\mathcal{M}_{01}$. The matroids $\mathcal{M}_o$ and $\mathcal{M}_{ab}$ with $(a,b) \neq (1,1)$ are representable over every large enough field. We skip the proof of this fact, but we present $\mathbb{F}_{11}$-linear representations for $\mathcal{M}_o$, $\mathcal{M}_{00}$, and $\mathcal{M}_{01}$, which are given, respectively, by the following matrices, whose columns are indexed as $(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)$.

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 6 & 0 & 1 & 0 & 4 & 0 & 2 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 5 & 0 & 1 & 1 & 0 & 10 \\ 1 & 0 & 8 & 1 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 6 & 7 & 0 \\ 1 & 5 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 7 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 7 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 9 & 0 & 7 & 6 & 0 & 3 & 6 & 0 & 6 \end{pmatrix}.$$

Let Γ be the port of the Tic-Tac-Toe matroid $\mathcal{M}$ at $p_o = (0,0)$. Let Γ_{11} be the port of $\mathcal{M}_o$ at p_o and, for $(a,b) \neq (1,1)$, let Γ_{ab} be the port of $\mathcal{M}_{ab}$ at p_o. Since they are ports of $\mathbb{F}_{11}$-linear matroids, each of the nine access structures Γ_{ab} admits an ideal $\mathbb{F}_{11}$-linear secret sharing scheme. Every qualified set of Γ is qualified in at least five of the six access structures Γ_{11}, Γ_{00}, Γ_{01}, Γ_{02}, Γ_{10}, and Γ_{20}. In addition, the unqualified sets of Γ are also unqualified in those six access structures. Therefore, by combining the ideal linear secret sharing schemes for those six access structures in a λ-decomposition with $\lambda = 5$, we obtain a linear secret sharing scheme for Γ with information ratio $6/5$. The reader is referred to [92, 105] for more information about λ-decompositions. □

5.4.1 Commments About the Lower Bounds

Farràs, Ribes-González, and Ricci [53] showed that given two access structures Γ and Γ', their optimal information ratios $\sigma(\Gamma)$ and $\sigma(\Gamma')$, have the following property

$$|\sigma(\Gamma) - \sigma(\Gamma')| \leq |\Gamma \cup \Gamma'| - |\Gamma \cap \Gamma'|.$$

Hence, for two access structures that differ by only one subset, their optimal information ratios can only be at a maximum distance one from each other. The implication of this in our work is that most of the bounds we might expect to get when dealing with ports of matroids on at most 9 points will not be too far from 1. This is because, for matroids

on $n \leq 9$ points, there is a healthy number of representable matroids among them, resulting in ideal access structures. And since some of the non-representable matroids are just a circuit-hyperplane derelaxation away from being representable (think Vámos), we have that their optimal information ratios, $\sigma(\Gamma)$ for the port of the representable matroid, and $\sigma(\Gamma')$ for the port of the non-representable matroid, are trivially bounded as $|1 - \sigma(\Gamma')| \leq |\Gamma \cup \Gamma'| - |\Gamma \cap \Gamma'| = 1$ implies $1 = \sigma(\Gamma) \leq \sigma(\Gamma') \leq 2$.

We should also note that this property holds when considering only $\kappa(\Gamma)$ or even restricting to linear schemes.

5.5 Secret Sharing for Sparse-Paving Matroids

Let $sp(n)$ and $m(n)$ represent, respectively, the number of sparse-paving matroids and all matroids on n elements. Mayhew and Welsh [88] showed that the number of sparse-paving matroids on n elements satisfies the following equation

$$\log\log sp(n) = n - (3/2)\log n + O(\log\log n)$$

and then conjectured that the same equality holds for $m(n)$. The conjecture was proved by Bansal et al. [11].

In order to study asymptotic properties, it is convenient to say that *almost all* elements in a family F have the property P, which means that the proportion of members of F that satisfy P is asymptotically as large as F itself, i.e.,

$$\lim_{n\to\infty} \frac{|F_P(n)|}{|F(n)|} = 1.$$

Mayhew et al. [85] conjectured that asymptotically, almost all matroids are sparse paving. The current best result in this direction is the following theorem, by Pendavingh and van der Pol [95].

Theorem 5.6 ([95])**.** $\lim_{n\to\infty} \frac{\log sp(n)}{\log m(n)} = 1$

Hence, results obtained for sparse-paving matroids could be quite significant for matroids in general.

A characteristic of ports of sparse-paving matroids is that the size of authorized and forbidden sets of their ports are tightly bounded. Since sparse paving matroids have that circuits have size between r and $r+1$ and cocircuits have size between r^* and r^*+1, where $r^* = n - r$, we have the following characterization of the ports of sparse-paving matroids.

Lemma 5.7. *Let $\mathcal{M}$ be a (r, n) sparse-paving matroid. Then all sets $A \subseteq Q$ such that $|A| < r - 1$ are forbidden, while all sets $B \subseteq Q$ such that $|B| > r + 1$ are authorized.*

Proof. $\mathcal{M}$ being paving implies minimal authorized sets are of size r or $r-1$. This means all sets A such that $|A| < r-1$ are forbidden. Now, let $\mathcal{M}^*$ be the dual of $\mathcal{M}$. Since $\mathcal{M}^*$ is also paving, its minimal authorized sets have size $r^* = n-r$ or $r^*-1 = n-r-1$. Thus all sets of size less than $r^* - 1$ are forbidden in $\mathcal{M}^*$. And since the dual of a forbidden

set is authorized in the dual access structure, we have that all sets of size greater than $n-(r^*-1)=r+1$ are authorized in $\mathcal{M}$. Hence, all sets $A \subseteq Q$ such that $|A| < r-1$ are forbidden, while all sets $B \subseteq Q$ such that $|B| > r+1$ are authorized in $\mathcal{M}$.

□

We introduce the notion of slice access structures from [15] as follows.

Definition 5.8. Let a, b be two integers satisfying $1 \leq a < b \leq n$. We define $S_{a,b}$ as the family of access structures Γ satisfying that, for every $A \subseteq Q$:

1. if $|A| > b$, then $A \in \Gamma$,
2. if $|A| < a$, then $A \notin \Gamma$.

Hence, from Lemma 5.7, we observe that ports of a (r, n) sparse-paving matroid are access structures in $S_{r-1,r+1}$.

5.5.1 Upper Bounds

We present upper bounds on the share size and the information ratio of secret sharing schemes for ports of sparse-paving matroids.

Theorem 5.9. *Ports of sparse-paving matroids on n points admit the following secret sharing schemes:*

1. *A scheme with secrets in $\mathbb{F}_2$ and share size $2^{O(\sqrt{n}\log n)}$.*
2. *An $(\mathbb{F}_2, 1)$-linear secret-sharing scheme with share size $2^{n/2+o(n)}$.*
3. *An $(\mathbb{F}_2, 2^{n^2})$-linear scheme with information ratio $2^{O(\sqrt{n\log n})}$.*

Proof. We present two main constructions for ports of sparse-paving matroids of rank r. First, we present a simple construction for matroids whose rank is small. It can also be used to construct schemes for matroids whose corank is small. Then, we present a construction based on the constructions in [15, 75] for the remaining matroids. In all these constructions, we only use the fact that ports of sparse-paving matroids of rank r are in $S_{r-1,r+1}$.

Let Γ be the port of a sparse-paving matroid of rank r. Suppose that $r = O(\sqrt{n/\log n})$. For this case, we consider a basic general linear scheme: we share the secret independently for every minimal authorized subset. Minimal authorized subsets are of size at most $r+2$, so every participant is in at most $\binom{n-1}{r+1}$ minimal authorized subsets. Hence, we obtain a scheme with information ratio at most $\binom{n-1}{r+1} \leq \left(\frac{e(n-1)}{r+1}\right)^{r+1} \leq 2^{O(\sqrt{n\log n})}$. Taking secrets of 1 bit, this scheme satisfies the first two bounds. If the secret has 2^{n^2} bits, we can take 2^{n^2} copies of this scheme, each one sharing one bit of the scheme. The resulting scheme is a $(\mathbb{F}_2, 2^{n^2})$-linear schemes with information ratio $2^{O(\sqrt{n\log n})}$.

Now suppose that $n-r = o(\sqrt{n/\log n})$. Then Γ^*, the dual of Γ, is in $S_{n-r-1,n-r+1}$. Since Γ^* is a port of a sparse-paving matroid satisfying the previous condition, Γ^* admits the

schemes presented above. Linear schemes for Γ^* can be transformed into linear schemes for Γ, maintaining the share size and the information ratio (see [92], for example).

Finally, suppose that the rank and co-rank of the matroid are $\omega(\sqrt{n/\log n})$. In this case, we construct secret sharing schemes using results and techniques in [15, 75].

Liu and Vaikuntanathan present in [75, Proof of Theorem 3.2] a secret sharing scheme for any access structure $\Gamma \in S_{a,b}$ with share size at most

$$\frac{\binom{n}{a}}{\binom{n/k}{a/k}^k}\binom{k}{b-a}2^{(b-a+1)n/k+O(\log n)}CDS, \tag{5.1}$$

where k is a parameter that divides n and $b-a \leq k$, and CDS is the computational complexity of a $(k-b+a)$-CDS protocol for a function defined from Γ (see [75] for more details). Computations in [75, Proof of Theorem 3.2] are optimized for the case $a = n/2 - \delta(n)$ and $b = n/2 + \delta(n)$, for $\delta(n) = o(n/logn)$. In our case, the setting is different: $a = r-1$ and $b = r+1$.

Now we approximate some factors of (5.1). Using the Stirling approximation of the binomial, we get that

$$\frac{\binom{n}{a}}{\binom{n/k}{a/k}^k} \sim \frac{1}{\sqrt{k}}\left(\frac{2\pi(n-a)a}{nk}\right)^{(k-1)/2} \tag{5.2}$$

Taking $k = \sqrt{\frac{n}{\log n}}$, this expression is upper bounded by $2^{O(\sqrt{n\log n})}$. Additionally, since $b-a=2$, $2^{(b-a+1)n/k} = 2^{O(\sqrt{n\log n})}$.

By [76, Proof of Lemma 3.13], there exists a CDS protocol for secrets in $\mathbb{F}_2$ with computational complexity at most $2^{O(\sqrt{\log X}\log\log X)}$, where $X \leq \binom{n/k}{a/k}^k \leq (\frac{en}{a})^a$. This value is smaller than $2^{O(\sqrt{a\log(n/a)}\log a)} \leq 2^{O(\sqrt{n}\log n)}$. Combining these approximations in (5.1) and the bound on the CDS computational complexity, we obtain share size $2^{O(\sqrt{n}\log n)}$.

For the second scheme, we use the linear scheme in [20, 76] with computational complexity $O(\binom{n/k}{a/k}^{k/2})$. The resulting scheme has share size $2^{n/2+o(n)}$. For the third scheme, we use the CDS protocols from [4] that have secrets of size 2^{n^2} and information ratio at most 4. □

Notice that approximations in (5.1) can be slightly improved for sparse-paving matroids with rank or corank $o(n)$. Also, using the first construction, the bound for $(\mathbb{F}_2, 1)$-linear schemes can be greatly improved for sparse-paving matroids with rank or corank $o(n)$.

The upper bounds in Theorem 5.9 are the same as the bounds for almost all access structures found in [15]. If the conjecture that almost all matroids are sparse paving is proven to be true, then the current upper bounds on the share size for ports of almost all matroids and almost all access structures will be the same.

5.5.2 Lower Bounds

In this section we present lower bounds on the share size and the information ratio of $(\mathbb{F}_q, 1)$-linear secret sharing schemes for ports of sparse-paving matroids. Since all these

bounds are obtained by means of counting arguments, these results also hold for almost all ports of matroids. In order to count the number of ports of sparse-paving matroids, we use the following lemma.

Lemma 5.10. *Let $|Q| = n$. The number of ports of sparse-paving matroids on Q is $2^{\Theta(2^n/n^{3/2})}$.*

Proof. By [47], the number of matroid ports is $2^{\Theta(2^n/n^{3/2})}$. The result holds by Theorem 5.6. □

For every finite field $\mathbb{F}_q$, almost all access structures require $(\mathbb{F}_q, 1)$-linear secret sharing schemes with information ratio $\Omega(2^{n/2-O(\log n \log\log q)})$ [7]. The same bound holds for almost all matroid ports [47], and can be extended to almost all sparse-paving matroids, as follows.

Theorem 5.11. *For every finite field $\mathbb{F}_q$ and integer $\ell > 0$, almost all ports of sparse-paving matroids require $(\mathbb{F}_q, \ell)$-linear secret sharing schemes of total information ratio*

$$\Omega\left(\frac{2^{n/2}}{n^{3/4}\ell\sqrt{\log q}}\right).$$

Proof. By [7, 47], the number of $(\mathbb{F}_q, \ell)$-linear secret sharing schemes of total information ratio at most t is smaller than $q^{\ell^2 t^2}$. Taking $t = c2^{n/2}/(n^{3/4}\ell\sqrt{\log q})$ with a small enough constant c, we see almost all ports of sparse-paving matroids require $(\mathbb{F}_q, \ell)$-linear schemes of total information ratio at most t. □

Now we present two more lower bounds. These bounds are direct consequences of counting arguments presented in [15].

Theorem 5.12. *For almost all ports of sparse-paving matroids Γ with n parties the following property holds: For every finite field $\mathbb{F}$, the total share size in every $(\mathbb{F}, 1)$-linear secret sharing scheme realizing Γ with a one-bit secret is at least $2^{n/2-o(n)}$.*

Proof. By [15, Theorem 3.11], the number of 1-linear secret-sharing schemes with total share size D is at most 2^{3D^2}. According to Lemma 5.10, almost all ports of sparse-paving matroids require total share size larger than $D = 2^{n/2}/n$. □

Theorem 5.13. *For almost all ports of sparse-paving matroids Γ with n parties the following property holds: For every finite field $\mathbb{F}$, the information ratio in every $(\mathbb{F}, 1)$-linear secret sharing scheme realizing Γ is at least $2^{n/3-o(n)}$.*

Proof. By [15, Theorem 3.10], the number of access structures that can be realized by a 1-linear secret sharing scheme with total information ratio is upper-bounded by $2^{d^3/2}$ According to Lemma 5.10, almost all ports of sparse-paving matroids require total information ratio larger than $d = 2^{n/3}/n^{2/3}$. The same bound also holds for the information ratio. □

So far, we presented lower bounds on the share size of $(\mathbb{F}_q, 1)$-linear schemes for matroid ports using different counting arguments. We dedicate the rest of the section to discuss other existing lower bounds.

General lower bounds for all access structures are better than the ones that are known for all matroid ports. This is due to the fact that the current best lower bound on the information ratio, which is $\Omega(n/\log n)$[36], was obtained using the LP method with Shannon inequalities. With this procedure, the lower bound obtained for matroid ports is always 1.

The current best lower bound on information ratio of secret sharing schemes for matroid ports is shown in Appendix B: for some ports of the F_8 matroid, which is a non-Ingleton-compliant matroid on 8 points, the share size has a lower bound of $8/7$.

There is a huge gap between the lower bounds for the information ratio of general linear schemes. The bound $n^{\Omega(\log n)}$ [14] was obtained using a method developed by Beimel, Gál and Paterson [16]. This method can also be applied to matroid ports but, as of now, there has been no success. The current best lower bound for general linear schemes for matroid ports is $4/3$, and it was obtained applying the LP method with the common information property. We add a proof of this bound in Appendix B.4.

The current best lower bound on the information ratio for $(\mathbb{F}_q, 1)$-linear schemes for general access structures is $2^{\Omega(n)}$ [97]. We do not know any explicit matroid port requiring information ratio $\omega(1)$.

Chapter 6

Conclusion and Future Work

Our main task for this thesis was to present a new tool for the study of matroid representation properties. We achieved this by developing a linear programming technique using the CI and AK information properties, which are properties satisfied by linear and almost entropic matroids, respectively. We showed the efficacy of these tools on "small" matroids (i.e., 8- and 9-point matroids). However, the problem with working with these tools at depths greater than 1 (or even at depth 1 for large matroids) is that they are rather computationally expensive ventures, even taking into consideration the optimizations we discussed in Section 3.7. Finding better optimizations for these tools will prove immensely useful when studying larger matroids or smaller matroids at deeper levels. We showed that CI is preserved by taking minors. Finding a similar result for AK and also if there are other matroid operations that preserve CI (and AK) is worth undertaking.

We also studied some other properties that are satisfied by linearly representable matroids. These are the so-called matroid intersection properties [9]: Levis, Euclidean, and generalized Euclidean intersection properties. We found that these properties could be checked at deeper levels than how they were initially conceived to find non-representable matroids, much like our notion of k-CI/AK-compliance for some positive integer k or the Ingleton-Main/Dress-Lovasz check at depth k of [28]. While we were able to show for rank-4 matroids the clear connection between CI and these intersection properties, the question for larger ranks is still open.

There is also a question of equivalence of these intersection properties. While it is known that all three intersection properties are equivalent for rank-4 matroids [9], we wonder if at some level, we might find something similar for rank-5 matroids or higher. Another open problem is to find if there are connections between the tools introduced in this thesis and other matroid extension properties like the Ingleton-Main and Dress-Lovasz extensions.

We worked on the characterization of all matroids on 8 points with respect to the representation properties. Mayhew and Royle [87] showed that there are only 5 Ingleton-compliant matroids on 8 ponts that are not linearly representable. In this thesis we showed that of these 5 matroids, 3 (P_1, P_2' and P_2'') are also not folded linear matroids while the other 2 are, thereby completing that characterization. However, we are not able to say if either or all of these 3 matroids are algebraic or even almost entropic. For these matroids neither CI nor AK were helpful at the basic level, i.e., at depth 1.

Solving these problems will complete the characterization of matroids on 8 points with respect to algebraicity and almost entropicity.

Using CI and the intersection properties, we found new families of Ingleton-compliant $(5, 9)$ matroids that are not folded linear. The first family, which we called TTT family, contains the Tic-Tac-Toe matroid. We analyzed properties of these matroids and determined the configuration of their circuit-hyperplanes that made them non-representable. We were able to show that this family extends to matroids on more than 9 points and with rank greater than 5. We also analyzed the duals of these matroids and found them to be non almost entropic—and hence, non-algebraic—due to 3-AK (Bollen [28] found them to be non-algebraic due to Ingleton-Main at depth 3). However, we could not say anything about the algebaicity of TTT matroids (some of them were found to be non-2-algebraic in [28]).

An interesting thing to note about TTT matroids and sparse-paving non-Ingleton-compliant matroids in general is that they have special configurations of their circuit-hyperplanes that prevent linear representability: the TTT configuration for the former and the Vámos configuration for the latter. We wonder if there are other "forbidden" configurations, perhaps for higher ranks, that prevent linear representability of matroids.

The second family of Ingleton-compliant non-representable matroids (Section 4.5.1) are similar to TTT matroids in all respects except one: they are non sparse-paving matroids. Again, Bollen [28] used the Frobenius flocks method to determine the non-algebraicity of many but not all of these matroids over fields of characteristic 2, so closing off this family with respect to algebraicity is still open.

The third family of non-linearly representable matroids we found is made up of 1-GP but non-2-EP Ingleton-compliant (5,9) matroids (Section 4.5.2). We found that members of this family are 1-CI. We were also able to show that most of them are not 2-CI, and hence non folded-linear matroids. However, while we were able to find all (5,9) members of the first two families, we were not able to do so for this family due to time constraints. We note that it is possible that some of the matroids we found may indeed be 2-CI. Also, there could be 1-CI but non-2-CI matroids we failed to capture. For all these matroids, their algebraicity is still open.

With respect to secret sharing, we extended the results of Farràs et al. [50] for matroid ports by finding bounds on the information ratio of secret sharing schemes for the ports of all 8-point matroids. We obtained new lower bounds on σ for the ports of the 39 non-Ingleton-compliant 8-point matroids and new bounds on λ for most of them. While we were able to improve the bound on σ for most of these matroids, we were not able to do so for λ. Furthermore, we found that all non-Ingleton-compliant sparse-paving matroids have a lower bound of at least $4/3$ on λ and $9/8$ on σ. We wonder if this separation result extends to non-Ingleton-compliant matroids that are not sparse paving. There's also a question of whether there are separation results for other matroid representation properties.

We found that ports of TTT matroids and also matroids in the second family of Ingleton-compliant non-1-GP matroids all had a non-trivial bound on λ. Considering that we are yet to find ports of any Ingleton-compliant 8-point matroid with a non-trivial bound, this would suggest that the ports of the Tic-Tac-Toe matroid might be one of the smallest such ports with non-trivial bounds on λ. Also, we were able to show that the $6/5$ bound on λ for one of the ports of the Tic-Tac-Toe matroid is tight by constructing a linear

scheme for it. However, these ports all had a trivial bound on σ. It might be possible to find non-trivial bounds on σ for these matroid ports, but considering that they are ports on 8 participants, the computational cost is currently prohibitive.

Seeing that we were able to improve the bounds on σ for some of the matroids we studied, we wonder just how far one can go to get improvements using the AK property. Moreover, one would like to see if combining the copy lemma with the AK property would yield even better results for secret sharing. In addition, the quest for improving the current best lower bound for secret sharing schemes, $\Omega(n/\log n)$ [36], is still on.

We also applied the CI and AK techniques to network coding. We studied the Vámos network but were not able to improve on the results currently available though we matched them. Finding ways to improve the techniques so as to obtain better bounds in network coding will be worthwhile.

We also studied general properties of the ports of sparse-paving matroids. We found upper bounds similar to those found for almost all access structures [15] and new lower bounds for linear schemes. In particular, we saw that ports of sparse-paving matroids admit secret sharing schemes with share size $2^{O(\sqrt{n}\log n)}$. Finding constructions such as this for matroid ports in general would also be good. In the case of general schemes, we were not able to find non-constant lower bounds on the information ratio. Hence, the question of whether matroid ports admit more efficient schemes in terms of share size than general access structures is still open.

UNIVERSITAT ROVIRA I VIRGILI
COMMON INFORMATION TECHNIQUES FOR THE STUDY OF MATROID REPRESENTATION AND SECRET SHARING SCHEMES
Michael Olugbenga Bamiloshin

Appendix A

TTT Matroids

A.1 Algebraicity of TTT Matroids

The 181 (5,9) TTT matroids with their 2-algebraic information are listed in Table A.1. The numbers given are the identifiers of these matroids in the Mayhew and Royle matroid database (the Bollen ids are in parenthesis [27]). Bollen [28] found that 62 of these are non 2-algebraic matroids due to their not being Frobenius-flock representable, while 10 of them, being Vámos matroids, are non 2-algebraic matroids due to Ingleton-Main, leaving 109 with undetermined 2-algebraic status. The relationship between the TTT matroids found to be non 2-algebraic and their TTT relaxations is shown in Fig. A.1. We also show the Vámos or P minors of these matroids where available (by P minors we mean: P_1, P_2', P_2'' and P_3). An interesting bit of information is that all 10 TTT-Vámos matroids have the same Vámos minor: 1509.

Matroid	2-Algebraic status	2-Algebraic certificate	Minor
265437 (44146)	False	2flock	P_2'', P_1
268016 (187730)	False	2flock	P_2''
280254 (101310)	—	—	P_3
275399 (95544)	—	—	—
274247 (184043)	—	—	P_3
265552 (93449)	False	2flock	P_3, P_1
269551 (135315)	False	2flock	P_2'', P_1
303175 (90881)	—	—	—
276341 (7517)	—	—	—
265420 (93442)	False	I-M condition	Vámos matroid, $1509, P_2', P_2'', P_1$
273141 (159715)	—	—	—
308279 (124226)	—	—	—
277673 (100260)	—	—	—
268774 (187224)	—	—	P_3
269550 (75459)	False	2flock	P_2', P_2'', P_1
267671 (139633)	—	—	P_2''
265014 (116990)	False	2flock	P_1

Table A.1 continued from previous page

Matroid	2-Algebraic status	2-Algebraic certificate	Minor
268805 (115941)	False	2flock	P_2''
351483 (152191)	—	—	—
308285 (10277)	—	—	—
328941 (122477)	—	—	—
277656 (78353)	—	—	—
303094 (58546)	—	—	—
273139 (101274)	—	—	—
265465 (73976)	False	2flock	P_2''
276671 (144442)	—	—	—
328917 (108734)	—	—	—
280733 (7746)	—	—	P_2''
265715 (73964)	False	2flock	P_1
269557 (139486)	False	I-M condition	Vámos matroid, $1509, P_2'$
280253 (161108)	—	—	P_3
283581 (159514)	—	—	—
269824 (74261)	—	—	—
268961 (187835)	—	—	P_2'
265008 (164114)	False	2flock	P_2', P_1
335557 (130851)	—	—	—
283626 (160605)	—	—	—
265129 (129143)	False	2flock	P_2', P_1
328928 (121151)	—	—	—
295231 (12377)	—	—	—
265601 (39125)	—	—	—
299721 (11521)	—	—	P_3
265409 (134986)	False	I-M condition	Vámos matroid, 1509
303095 (89912)	—	—	—
283624 (175047)	—	—	P_2'
280246 (16670)	—	—	—
274066 (161491)	False	2flock	P_2''
276792 (102470)	—	—	P_2''
265451 (44128)	False	I-M condition	Vámos matroid, $1509, P_2', P_1$
269559 (164468)	False	2flock	P_3, P_1
304067 (90597)	—	—	—
268765 (187743)	False	2flock	P_2''
277240 (183200)	—	—	—
265421 (43998)	False	2flock	P_2', P_1
267946 (75461)	—	—	P_1
293361 (82200)	—	—	—
269895 (139329)	False	2flock	—
270130 (168724)	—	—	—
327157 (119019)	—	—	—
265760 (8796)	False	2flock	P_2', P_2''
303158 (173935)	—	—	P_2''

Table A.1 continued from previous page

Matroid	2-Algebraic status	2-Algebraic certificate	Minor
308385 (37104)	—	—	—
308386 (37098)	—	—	—
327043 (24938)	—	—	—
265551 (80260)	False	2flock	P_2'', P_1
306452 (36769)	—	—	—
275394 (102491)	—	—	P_2''
275391 (7757)	—	—	P_2''
264999 (20015)	False	I-M condition	Vámos matroid, $1509, P_2', P_2''$
282270 (101368)	False	2flock	—
275082 (183037)	—	—	P_3
282271 (100768)	—	—	—
280241 (101674)	—	—	—
304062 (174117)	—	—	—
265622 (44145)	False	2flock	P_2'', P_1
267678 (97430)	False	2flock	P_2'', P_1
268611 (115943)	False	2flock	P_2''
268018 (166668)	—	—	P_2', P_2''
268120 (115907)	False	2flock	—
293346 (82241)	—	—	—
281004 (161492)	—	—	P_2''
268017 (157004)	—	—	P_2', P_2''
265020 (134166)	False	2flock	P_2'', P_3, P_1
275398 (7766)	—	—	P_2''
266948 (187323)	False	2flock	P_2''
268958 (187834)	—	—	P_2'
265423 (44141)	False	2flock	P_2', P_2'', P_1
350495 (148386)	—	—	—
264994 (20018)	False	2flock	P_2', P_1
265270 (39134)	False	2flock	P_2'', P_3
264984 (164117)	False	2flock	P_2', P_1
308381 (46662)	—	—	—
265012 (116992)	False	2flock	P_2', P_1
265026 (43901)	False	2flock	P_2', P_2'', P_1
275410 (144406)	—	—	P_2''
301018 (128057)	—	—	—
265696 (81269)	False	2flock	P_2', P_1
327134 (41018)	—	—	—
281572 (34611)	—	—	P_1
319504 (180643)	—	—	—
269061 (59580)	—	—	—
328818 (118546)	—	—	—
280249 (159694)	—	—	P_3

Table A.1 continued from previous page

Matroid	2-Algebraic status	2-Algebraic certificate	Minor
300831 (126188)	—	—	—
267871 (75460)	—	—	P_1
264956 (49336)	False	2flock	P_2', P_1
265237 (93456)	False	2flock	P_2'', P_1
268613 (115939)	False	2flock	P_2''
320838 (130755)	—	—	—
275416 (96331)	—	—	P_2''
268099 (156140)	False	2flock	P_2''
280891 (102402)	—	—	—
265623 (44142)	False	2flock	P_1
281568 (96604)	—	—	P_1
304085 (154928)	—	—	P_2''
269704 (139638)	—	—	P_2''
308280 (12255)	—	—	—
294990 (82743)	—	—	—
291383 (124364)	—	—	—
264950 (45969)	False	2flock	P_1
281581 (154226)	—	—	—
351377 (62136)	—	—	—
276430 (102490)	—	—	P_2''
268486 (156761)	—	—	P_3
269060 (156409)	—	—	—
292609 (126263)	—	—	—
328810 (106019)	—	—	—
335558 (130868)	—	—	—
268272 (59410)	—	—	P_3
264952 (94190)	False	I-M condition	Vámos matroid, 1509, P_1
283630 (7805)	—	—	—
267672 (139609)	False	2flock	P_1
280230 (55342)	—	—	P_2''
368054 (185672)	—	—	—
264978 (164115)	False	2flock	P_1
273582 (96423)	—	—	—
328817 (189486)	—	—	—
275411 (6346)	False	2flock	—
283632 (161684)	—	—	P_2'
268115 (156884)	False	2flock	P_2''
282272 (160978)	—	—	—
293347 (15656)	—	—	—
265553 (93405)	False	2flock	P_3
281794 (154211)	—	—	P_1
268475 (166667)	False	2flock	P_3
266923 (187302)	False	2flock	—
351471 (62109)	—	—	—
299715 (15603)	—	—	—

Table A.1 continued from previous page

Matroid	2-Algebraic status	2-Algebraic certificate	Minor
267669 (75448)	False	2flock	P_2'', P_1
265555 (93409)	False	2flock	P_3, P_1
265556 (129144)	False	2flock	P_2'', P_1
265011 (134161)	False	I-M condition	Vámos matroid, $1509, P_1$
267675 (58047)	False	2flock	P_1
268477 (156699)	—	—	P_3
283631 (7795)	—	—	—
265262 (73958)	False	2flock	P_2', P_2'', P_1
265468 (44123)	False	2flock	P_2'', P_1
268474 (187780)	False	2flock	P_2''
264955 (96550)	False	2flock	P_1
266399 (164462)	False	2flock	P_1
265602 (39107)	—	—	P_2'
267873 (58043)	False	I-M condition	Vámos matroid, $1509, P_1$
268476 (156184)	—	—	P_2', P_3
265424 (93463)	—	—	P_2'
275417 (7684)	—	—	—
281574 (135443)	False	I-M condition	Vámos matroid, 1509
265547 (80265)	False	2flock	P_1
270133 (139551)	—	—	P_1
300609 (11572)	—	—	—
265018 (116991)	False	2flock	P_2', P_1
304066 (89377)	—	—	—
267897 (164481)	—	—	—
269062 (156905)	False	2flock	P_2'', P_3
303086 (103366)	—	—	—
269558 (135319)	False	2flock	P_2', P_1
265695 (93468)	False	I-M condition	Vámos matroid, 1509
265023 (166567)	False	2flock	P_2''
265389 (134987)	False	2flock	P_2'', P_1
265422 (73962)	False	2flock	P_2', P_2'', P_3, P_1
303165 (173915)	—	—	P_2''
265028 (43902)	False	2flock	P_1

Table A.1: All 181 (5,9) TTT Matroids

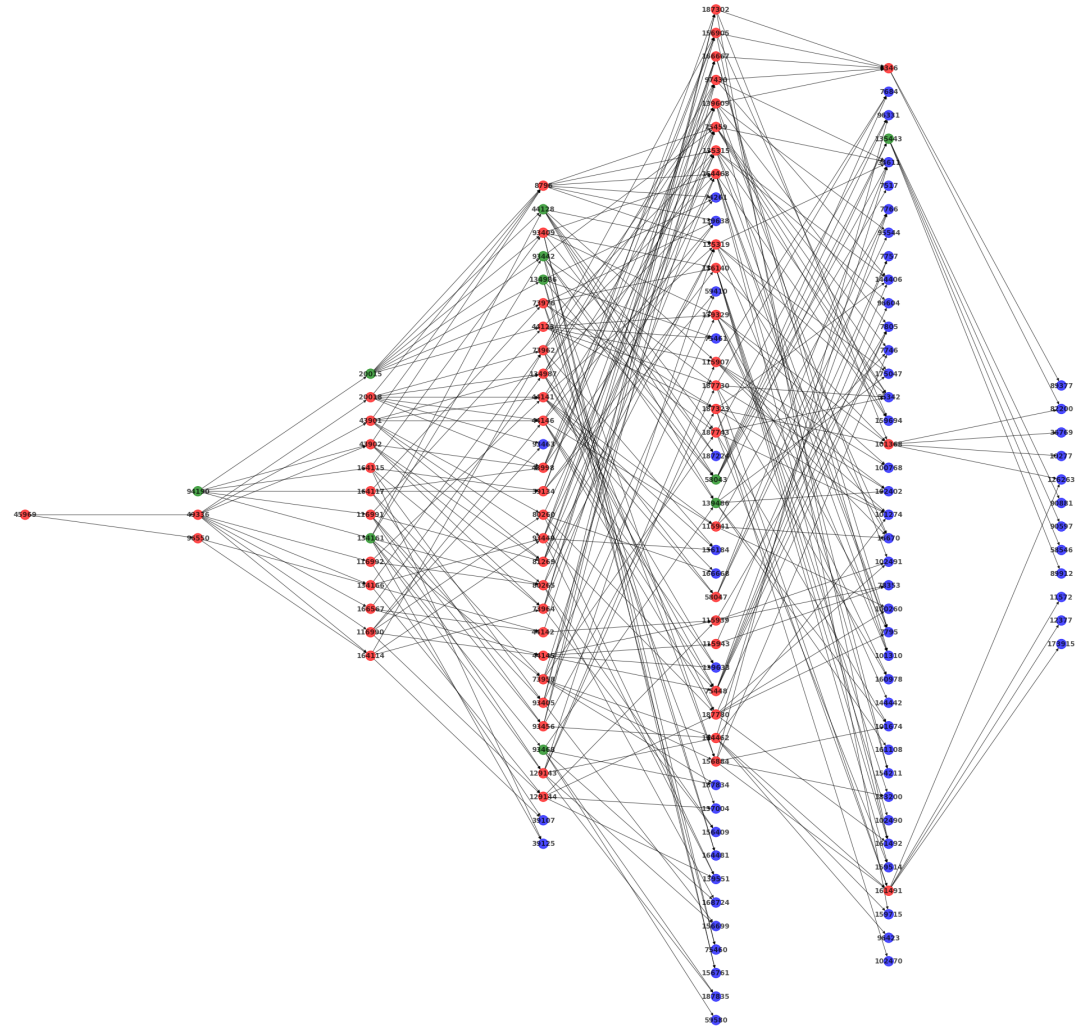


FIGURE A.1: Confirmed Non 2-Algebraic $(5, 9)$ TTT matroids With Their TTT Relaxations

Appendix B

Bounds for Secret Sharing

B.1 Bounds for Matroids on 8 Points

Table B.1 contains the results of our computations on the non-Ingleton-compliant 8-point matroids and is described as follows. The names/numbers of the matroids are as they appear in [87] (which coincides with the SAGE database of matroids). The ports of each matroid were first obtained and then ran through a program that identifies isomorphic ports. These were then noted and excluded from the subsequent checks knowing that whatever results were obtained for the ports to which they were isomorphic to would also apply to them. By applying Linear Programming Problem 7 to the ports of these matroids, we obtained the lower bound $9/8 \leq \sigma(\Gamma)$. It was possible to improve this lower bound in the case of some of the ports via a once-repeated application of the Linear Programming Problem. These improved lower bounds are what appear in the column marked *"Improved bound on $\sigma(\Gamma)$"*. Applying Linear Programming Problem 6 to all the ports gave the lower bound $4/3 \leq \lambda(\Gamma)$. However, unlike in the case of $\sigma(\Gamma)$, we were not able to improve this bound on $\lambda(\Gamma)$ for any of the ports of the matroids studied.

Matroid	Port	Improved bound on $\sigma(\Gamma)$
1490	0, 2, 3, 4, 5, 6	8/7
1491	0, 3, 7	33/29
1491	2, 4, 5, 6	8/7
1492	0, 1, 2, 3, 4, 5, 6, 7	49/43
1494	3, 4, 5, 6	33/29
1499	0, 2, 3, 4, 5, 6	8/7
1500	0, 2, 3, 4, 5, 6	8/7
1501	0, 1, 2, 3, 6, 7	33/29
1501	4, 5	8/7
1502	5, 6	8/7
1502	2, 3, 4, 7	33/29
1508	3, 4, 5, 6	33/29
1509	3, 4, 5, 6	33/29
1510	3, 4, 5, 6	33/29
1518	3, 4, 5, 6	33/29
1520	2, 3, 4, 7	33/29

Table B.1 continued from previous page

Matroid	Port	Improved bound on $\sigma(\Gamma)$
1524	3, 4, 5, 6	33/29
1525	0, 2, 4, 5	33/29
1525	3, 6	8/7
1526	0, 2, 3, 4, 5, 6	8/7
1527	0, 2, 4, 5	33/29
1528	0, 2, 3, 6	8/7
1529	1, 4, 5, 7	33/29
1531	2, 5, 6, 7	33/29
1532	4, 7	8/7
1532	0, 1, 2, 3, 5, 6	33/29
1549	3, 4, 5, 6	33/29
1568	3, 4, 5, 6	33/29
1572	2, 3, 4, 7	33/29
1576	3, 4, 5, 6	33/29
1578	3, 4, 5, 6	33/29
1579	0, 2, 4, 5	33/29
1579	3, 6	8/7
1580	0, 2, 3, 6	33/29
1641	3, 4, 5, 6	33/29
1646	2, 5, 6, 7	33/29
1654	3, 4, 5, 6	33/29
1656	0, 2, 3, 6	33/29
1657	0, 2, 3, 6	33/29
1660	0, 2, 3, 6	33/29
$AG(3,2)'$	1, 3, 5, 7	49/43
F_8	1, 7	8/7
F_8	3, 4, 5, 6	33/29
Q_8	1, 4, 6, 7	49/43
V_8^+	0, 2, 3, 6	33/29
V_8	2, 3, 6, 7	33/29[1]

TABLE B.1: Bounds for 8-point Matroids

B.2 Bounds for Matroids on 9 Points

The results of our computations on matroids on 9 points are presented in Tables B.2 and B.3. Like in Table B.1, the numbers of the matroids in Tables B.2 and B.3 are as they appear in [87]. Considering that this is a much larger family of matroids compared to those on 8 points, what we did here was to randomly select a number of matroids from this family and check if they were Ingleton-compliant matroids. For the ones that were not Ingleton-compliant, we extracted their ports and then applied Linear Programming Problem 6 to the ports. By doing this we were able to obtain lower bounds on $\lambda(\Gamma)$. These bounds are listed in the column marked *"Bound on* $\lambda(\Gamma)$*"*. While we obtained

[1]Improved in [58]

the bound $4/3 \leq \lambda(\Gamma)$ for majority of the ports, thereby coinciding with what we got for the matroids on 8 points, a few of them resulted in new bounds 7/6 and 6/5.

Matroid	Port	Bound on $\lambda(\Gamma)$
148786	0, 1, 3, 4, 5, 6, 7, 8	4/3
148786	2	6/5
148788	0, 1, 3, 4, 5, 6, 7, 8	4/3
148788	2	6/5
148789	0, 1, 3, 4, 5, 6, 7, 8	4/3
148789	2	6/5
148790	0, 1, 3, 4, 5, 6, 7, 8	4/3
148790	2	6/5
149196	0, 1, 2, 3, 4, 5, 6, 7, 8	4/3
149197	0, 1, 2, 3, 4, 5, 6, 7, 8	4/3
149202	0, 1, 2, 3, 4, 5, 7, 8	4/3
149202	6	6/5
149206	0, 1, 3, 4, 5, 6, 7, 8	4/3
149206	2	7/6
149505	0, 1, 2, 4, 5, 6, 7, 8	4/3
149505	3	6/5
92675	0, 1, 2, 3, 4, 5, 7, 8	4/3
92675	6	7/6
92678	0, 1, 2, 3, 4, 5, 7, 8	4/3
92678	6	6/5
92993	0, 1, 2, 3, 4, 5, 7, 8	4/3
92993	6	7/6
93159	1, 2, 3, 4, 5, 6, 7, 8	4/3
93159	0	7/6
93160	1, 2, 3, 4, 5, 6, 7, 8	4/3
93160	0	7/6
93339	0, 1, 2, 3, 4, 5, 7, 8	4/3
93339	6	6/5
93634	0, 1, 2, 3, 4, 5, 7, 8	4/3
93634	6	7/6
93640	0, 1, 2, 3, 4, 5, 7, 8	4/3
93640	6	7/6
93644	0, 1, 2, 3, 5, 6, 7, 8	4/3
93644	4	6/5
93649	0, 1, 2, 3, 4, 5, 7, 8	4/3
93649	6	7/6
93650	0, 1, 2, 3, 4, 5, 7, 8	4/3
93650	6	6/5
93651	0, 1, 2, 3, 4, 5, 7, 8	4/3
93651	6	6/5
93652	0, 1, 2, 3, 4, 5, 6, 7, 8	4/3
93653	0, 1, 2, 3, 4, 5, 7, 8	4/3
93653	6	7/6

TABLE B.2: Bounds for Selected rank-4 9-point Matroids

Matroid	Port	Bound on $\lambda(\Gamma)$
293005	0, 1, 2, 3, 4, 6, 7, 8	4/3
293005	5	7/6
293447	1, 2, 3, 4, 5, 6, 7, 8	4/3
293447	0	7/6
305136	0, 1, 2, 3, 4, 5, 6, 7	4/3
305136	8	7/6
305478	0, 2, 3, 4, 5, 6, 7, 8	4/3
305478	1	6/5
324692	0, 1, 2, 3, 4, 5, 6, 7	4/3
324692	8	6/5
324822	0, 1, 2, 3, 4, 5, 6, 7	4/3
324822	8	6/5
294993	0, 1, 3, 4, 5, 6, 7, 8	4/3
294993	2	7/6
294994	0, 1, 3, 4, 5, 6, 7, 8	4/3
294994	2	6/5
295008	0, 1, 3, 4, 5, 6, 7, 8	4/3
295008	2	7/6
295009	0, 1, 3, 4, 5, 6, 7, 8	4/3
295009	2	7/6
295010	0, 1, 3, 4, 5, 6, 7, 8	4/3
295010	2	7/6
295012	0, 1, 2, 3, 4, 5, 7, 8	4/3
295012	6	7/6
295319	0, 1, 2, 3, 4, 5, 6, 7	4/3
295319	8	6/5
295320	0, 1, 2, 3, 4, 5, 6, 7	4/3
295320	8	6/5
295829	0, 1, 2, 4, 5, 6, 7, 8	4/3
295829	3	7/6
295831	0, 1, 2, 4, 5, 6, 7, 8	4/3
295831	3	7/6
323590	0, 1, 2, 3, 4, 6, 7, 8	4/3
323590	5	7/6
323602	0, 1, 2, 3, 4, 6, 7, 8	4/3
323602	5	6/5
370388	0, 2, 3, 4, 5, 6, 7, 8	4/3
370388	1	7/6

TABLE B.3: Bounds for Selected rank-5 9-point Matroids

B.3 Bounds for IC non-GP (5,9) Matroids

Here we present bounds on the ports of the Ingleton-compliant non-GP (5,9) matroids. While most of these matroid ports have a 6/5 bound on λ, a few ports have a 7/6 bound. We know that all the (5,9) TTT matroids are 1-AK-compliant matroids, but we do not

know if this is the same for the other matroids in this group. As such, we present only bounds on λ.

Matroid	Port	Bound on $\lambda(\Gamma)$
199553	$0,1,2,5,6,7,8$	6/5
199553	$3,4$	7/6
199807	$0,1,2,3,4,5,8$	6/5
199807	$6,7$	7/6
200470	$0,1,2,3,4,5,8$	6/5
200470	$6,7$	7/6
200589	$0,1,2,4,5,6,8$	6/5
200589	$3,7$	7/6
200633	$0,1,2,3,4,5,6,7,8$	6/5
200972	$0,1,2,4,5,7,8$	6/5
200972	$3,6$	7/6
201001	$0,1,2,3,5,6,8$	6/5
201001	$4,7$	7/6
201056	$0,1,2,3,4,5,8$	6/5
201056	$6,7$	7/6
201121	$0,1,3,4,5,6,7,8$	6/5
201121	2	7/6
201124	$0,1,2,3,4,5,6,7,8$	6/5
201827	$0,1,2,4,5,6,8$	6/5
201827	$3,7$	7/6
201869	$0,1,2,4,5,7,8$	6/5
201869	$3,6$	7/6
201957	$0,1,2,3,4,5,8$	6/5
201957	$6,7$	7/6
201958	$0,1,2,3,4,5,8$	6/5
201958	$6,7$	7/6
202832	$0,1,2,4,5,6,8$	6/5
202832	$3,7$	7/6
204059	$0,1,2,4,5,6,7,8$	6/5
204059	3	7/6
204585	$0,1,2,3,4,5,6,7,8$	6/5
204624	$0,1,2,4,6,7,8$	6/5
204624	$3,5$	7/6
204630	$0,1,2,4,6,7,8$	6/5
204630	$3,5$	7/6
204769	$0,1,2,3,4,5,6,7,8$	6/5
204896	$0,1,2,3,4,5,7,8$	6/5
204896	6	7/6
204903	$0,1,2,3,4,5,7,8$	6/5
204903	6	7/6
204973	$0,1,2,3,4,5,6,7,8$	6/5
205074	$0,1,2,3,4,5,6,7,8$	6/5
205111	0	7/6
205111	$1,2,3,4,5,6,7,8$	6/5
206383	$0,1,2,4,6,7,8$	6/5
206383	$3,5$	7/6

Table B.4 continued from previous page

Matroid	Port	Bound on $\lambda(\Gamma)$
206385	$0,1,2,4,6,7,8$	$6/5$
206385	$3,5$	$7/6$
206515	$0,1,2,3,4,5,6,7,8$	$6/5$
206844	$0,1,2,3,4,5,6,7,8$	$6/5$
206959	$0,1,2,3,4,5,6,7,8$	$6/5$
206992	$0,1,2,3,4,5,7,8$	$6/5$
206992	6	$7/6$
207536	$0,1,2,3,4,6,7,8$	$6/5$
207536	5	$7/6$
207550	$0,1,2,3,4,5,6,7,8$	$6/5$
207669	$0,1,2,3,4,5,6,7,8$	$6/5$
208093	$0,1,2,3,5,6,7,8$	$6/5$
208093	4	$7/6$
211135	$0,1,2,3,4,5,6,7,8$	$6/5$
211841	$0,1,2,3,4,5,7,8$	$6/5$
211841	6	$7/6$
211983	$0,1,2,3,4,7,8$	$6/5$
211983	$5,6$	$7/6$
211985	$0,1,2,3,4,5,6,7,8$	$6/5$
216857	$0,1,2,3,4,5,6,7,8$	$6/5$
217478	$0,1,2,3,4,5,6,7,8$	$6/5$
217597	0	$7/6$
217597	$1,2,3,4,5,6,7,8$	$6/5$
217772	$0,1,2,3,4,5,6,8$	$6/5$
217772	7	$7/6$
217846	$0,1,2,3,4,5,6,7,8$	$6/5$
218082	0	$7/6$
218082	$1,2,3,4,5,6,7,8$	$6/5$
218124	$0,1,2,3,4,5,6,7,8$	$6/5$
218129	$0,1,2,3,4,5,6,7,8$	$6/5$
218179	$0,1,2,3,5,6,7,8$	$6/5$
218179	4	$7/6$
218341	$0,1,2,3,4,5,6,8$	$6/5$
218341	7	$7/6$
220346	$0,1,2,3,4,5,6,8$	$6/5$
220346	7	$7/6$
220524	$0,1,2,3,4,5,6,7,8$	$6/5$
220657	$0,1,2,3,4,5,6,7,8$	$6/5$
221002	$0,1,2,3,4,5,6,8$	$6/5$
221002	7	$7/6$
221046	$0,1,2,3,4,5,6,7,8$	$6/5$
221323	$0,1,2,3,4,5,6,8$	$6/5$
221323	7	$7/6$
221541	$0,1,2,3,4,5,6,8$	$6/5$
221541	7	$7/6$
221542	$0,1,2,3,4,5,6,8$	$6/5$
221542	7	$7/6$

Table B.4 continued from previous page

Matroid	Port	Bound on $\lambda(\Gamma)$
221635	$0,1,2,3,4,5,7,8$	6/5
221635	6	7/6
221647	$0,1,2,3,4,6,7,8$	6/5
221647	5	7/6
221650	0	7/6
221650	$1,2,3,4,5,6,7,8$	6/5
221722	$0,1,2,3,4,5,6,7,8$	6/5
221834	$0,1,2,3,4,5,6,7,8$	6/5
221905	$0,1,2,3,4,5,6,7,8$	6/5
221910	$0,1,2,3,4,5,7,8$	6/5
221910	6	7/6
222035	$0,1,2,3,4,5,6,7,8$	6/5
222041	$0,1,2,3,4,5,6,8$	6/5
222041	7	7/6
222044	$0,1,2,3,4,5,6,7,8$	6/5
222384	$0,1,2,3,4,5,6,8$	6/5
222384	7	7/6
222385	$0,1,2,3,4,5,6,8$	6/5
222385	7	7/6
222436	$0,1,2,3,4,5,6,7,8$	6/5
223015	$0,1,2,3,4,5,6,8$	6/5
223015	7	7/6
223016	$0,1,2,3,4,5,6,8$	6/5
223016	7	7/6
223035	$0,1,2,3,4,5,6,7,8$	6/5
223221	$0,1,2,3,4,5,6,7,8$	6/5
223417	$0,1,2,3,4,5,6,7,8$	6/5
227084	$0,1,2,3,4,5,6,7,8$	6/5
227086	$0,1,2,3,4,5,6,7,8$	6/5
227789	$0,1,2,3,4,5,6,8$	6/5
227789	7	7/6
227977	$0,1,2,3,4,5,6,7,8$	6/5
228317	$0,1,2,3,4,5,7,8$	6/5
228317	6	7/6
228452	$0,1,2,3,4,5,6,7,8$	6/5
229354	$0,1,2,3,4,5,6,8$	6/5
229354	7	7/6
229356	$0,1,2,3,4,5,6,8$	6/5
229356	7	7/6
229357	$0,1,2,3,4,5,6,8$	6/5
229357	7	7/6
229741	$0,1,2,3,4,5,7,8$	6/5
229741	6	7/6
229892	0	7/6
229892	$1,2,3,4,5,6,7,8$	6/5
230229	$0,1,2,3,4,5,6,7,8$	6/5
230558	$0,1,2,3,4,5,6,7,8$	6/5

Table B.4 continued from previous page

Matroid	Port	Bound on $\lambda(\Gamma)$
231565	$0,1,2,3,4,5,6,8$	6/5
231565	7	7/6
231566	$0,1,2,3,4,5,6,8$	6/5
231566	7	7/6
231587	$0,1,2,3,4,5,6,7,8$	6/5
231588	$0,1,2,3,4,5,6,7,8$	6/5
231997	$0,1,2,3,4,5,6,7,8$	6/5
232065	$0,1,2,3,4,5,6,7,8$	6/5
232651	$0,1,2,3,4,5,7,8$	6/5
232651	6	7/6
232654	$0,1,2,3,4,5,7,8$	6/5
232654	6	7/6
232824	$0,1,2,3,4,5,6,7,8$	6/5
233072	$0,1,2,3,4,5,6,7,8$	6/5
233153	$0,1,2,3,4,5,6,7,8$	6/5
233156	$0,1,2,3,4,5,6,7,8$	6/5
233245	$0,1,2,3,4,5,7,8$	6/5
233245	6	7/6
233261	$0,1,2,3,4,5,7,8$	6/5
233261	6	7/6
241344	$0,1,2,3,4,5,6,8$	6/5
241344	7	7/6
241614	$0,1,2,3,4,5,7,8$	6/5
241614	6	7/6
243049	$0,1,2,3,4,5,6,7,8$	6/5
243792	$0,1,2,3,4,5,7,8$	6/5
243792	6	7/6
243800	$0,1,2,3,4,5,7,8$	6/5
243800	6	7/6
243801	$0,1,2,3,4,5,7,8$	6/5
243801	6	7/6
244422	$0,1,2,3,4,5,6,7,8$	6/5
244449	$0,1,2,3,4,5,6,7,8$	6/5
245708	$0,1,2,3,4,5,6,7,8$	6/5
245732	$0,1,2,3,4,5,6,7,8$	6/5
245765	$0,1,2,3,4,5,6,7,8$	6/5
253254	$0,1,2,3,4,5,7,8$	6/5
253254	6	7/6
253828	$0,1,2,3,4,5,6,7,8$	6/5
264950	$0,1,2,3,4,5,6,7,8$	6/5
264955	$0,1,2,3,4,5,6,7,8$	6/5
264956	$0,1,2,3,4,5,6,7,8$	6/5
264978	$0,1,2,3,4,5,6,7,8$	6/5
264984	$0,1,2,3,4,5,6,7,8$	6/5
264994	$0,1,2,3,4,5,6,7,8$	6/5
265008	$0,1,2,3,4,5,6,7,8$	6/5
265012	$0,1,2,3,4,5,6,7,8$	6/5

Table B.4 continued from previous page

Matroid	Port	Bound on $\lambda(\Gamma)$
265014	$0,1,2,3,4,5,6,7,8$	6/5
265018	$0,1,2,3,4,5,6,7,8$	6/5
265020	$0,1,2,3,4,5,6,7,8$	6/5
265023	$0,1,2,3,4,5,6,7,8$	6/5
265026	$0,1,2,3,4,5,6,7,8$	6/5
265028	$0,1,2,3,4,5,6,7,8$	6/5
265129	$0,1,2,3,4,5,6,7,8$	6/5
265237	$0,1,2,3,4,5,6,7,8$	6/5
265262	$0,1,2,3,4,5,6,7,8$	6/5
265270	$0,1,2,3,4,5,6,7,8$	6/5
265389	$0,1,2,3,4,5,6,7,8$	6/5
265421	$0,1,2,3,4,5,6,7,8$	6/5
265422	$0,1,2,3,4,5,6,7,8$	6/5
265423	$0,1,2,3,4,5,6,7,8$	6/5
265424	$0,1,2,3,4,5,6,7,8$	6/5
265437	$0,1,2,3,4,5,6,7,8$	6/5
265465	$0,1,2,3,4,5,6,7,8$	6/5
265468	$0,1,2,3,4,5,6,7,8$	6/5
265547	$0,1,2,3,4,5,6,7,8$	6/5
265551	$0,1,2,3,4,5,6,7,8$	6/5
265552	$0,1,2,3,4,5,6,7,8$	6/5
265553	$0,1,2,3,4,5,6,7,8$	6/5
265555	$0,1,2,3,4,5,6,7,8$	6/5
265556	$0,1,2,3,4,5,6,7,8$	6/5
265601	$0,1,2,3,4,5,6,7,8$	6/5
265602	$0,1,2,3,4,5,6,7,8$	6/5
265622	$0,1,2,3,4,5,6,7,8$	6/5
265623	$0,1,2,3,4,5,6,7,8$	6/5
265696	$0,1,2,3,4,5,6,7,8$	6/5
265715	$0,1,2,3,4,5,6,7,8$	6/5
265760	$0,1,2,3,4,5,6,7,8$	6/5
266399	$0,1,2,3,4,5,6,7,8$	6/5
266923	$0,1,2,3,4,5,6,7,8$	6/5
266948	$0,1,2,3,4,5,6,7,8$	6/5
267669	$0,1,2,3,4,5,6,7,8$	6/5
267671	$0,1,2,3,4,5,6,7,8$	6/5
267672	$0,1,2,3,4,5,6,7,8$	6/5
267675	$0,1,2,3,4,5,6,7,8$	6/5
267678	$0,1,2,3,4,5,6,7,8$	6/5
267871	$0,1,2,3,4,5,6,7,8$	6/5
267897	$0,1,2,3,4,5,6,7,8$	6/5
267946	$0,1,2,3,4,5,6,7,8$	6/5
268016	$0,1,2,3,4,5,6,7,8$	6/5
268017	$0,1,2,3,4,5,6,7,8$	6/5
268018	$0,1,2,3,4,5,6,7,8$	6/5
268099	$0,1,2,3,4,5,6,7,8$	6/5
268115	$0,1,2,3,4,5,6,7,8$	6/5

Table B.4 continued from previous page

Matroid	Port	Bound on $\lambda(\Gamma)$
268120	$0,1,2,3,4,5,6,7,8$	$6/5$
268272	$0,1,2,3,4,5,6,7,8$	$6/5$
268474	$0,1,2,3,4,5,6,7,8$	$6/5$
268475	$0,1,2,3,4,5,6,7,8$	$6/5$
268476	$0,1,2,3,4,5,6,7,8$	$6/5$
268477	$0,1,2,3,4,5,6,7,8$	$6/5$
268486	$0,1,2,3,4,5,6,7,8$	$6/5$
268611	$0,1,2,3,4,5,6,7,8$	$6/5$
268613	$0,1,2,3,4,5,6,7,8$	$6/5$
268765	$0,1,2,3,4,5,6,7,8$	$6/5$
268774	$0,1,2,3,4,5,6,7,8$	$6/5$
268805	$0,1,2,3,4,5,6,7,8$	$6/5$
268958	$0,1,2,3,4,5,6,7,8$	$6/5$
268961	$0,1,2,3,4,5,6,7,8$	$6/5$
269060	$0,1,2,3,4,5,6,7,8$	$6/5$
269061	$0,1,2,3,4,5,6,7,8$	$6/5$
269062	$0,1,2,3,4,5,6,7,8$	$6/5$
269550	$0,1,2,3,4,5,6,7,8$	$6/5$
269551	$0,1,2,3,4,5,6,7,8$	$6/5$
269558	$0,1,2,3,4,5,6,7,8$	$6/5$
269559	$0,1,2,3,4,5,6,7,8$	$6/5$
269704	$0,1,2,3,4,5,6,7,8$	$6/5$
269824	$0,1,2,3,4,5,6,7,8$	$6/5$
269895	$0,1,2,3,4,5,6,7,8$	$6/5$
270130	$0,1,2,3,4,5,6,7,8$	$6/5$
270133	$0,1,2,3,4,5,6,7,8$	$6/5$
273139	$0,1,2,3,4,5,6,7,8$	$6/5$
273141	$0,1,2,3,4,5,6,7,8$	$6/5$
273582	$0,1,2,3,4,5,6,7,8$	$6/5$
274066	$0,1,2,3,4,5,6,7,8$	$6/5$
274247	$0,1,2,3,4,5,6,7,8$	$6/5$
275082	$0,1,2,3,4,5,6,7,8$	$6/5$
275391	$0,1,2,3,4,5,6,7,8$	$6/5$
275394	$0,1,2,3,4,5,6,7,8$	$6/5$
275398	$0,1,2,3,4,5,6,7,8$	$6/5$
275399	$0,1,2,3,4,5,6,7,8$	$6/5$
275410	$0,1,2,3,4,5,6,7,8$	$6/5$
275411	$0,1,2,3,4,5,6,7,8$	$6/5$
275416	$0,1,2,3,4,5,6,7,8$	$6/5$
275417	$0,1,2,3,4,5,6,7,8$	$6/5$
276341	$0,1,2,3,4,5,6,7,8$	$6/5$
276430	$0,1,2,3,4,5,6,7,8$	$6/5$
276671	$0,1,2,3,4,5,6,7,8$	$6/5$
276792	$0,1,2,3,4,5,6,7,8$	$6/5$
277240	$0,1,2,3,4,5,6,7,8$	$6/5$
277656	$0,1,2,3,4,5,6,7,8$	$6/5$
277673	$0,1,2,3,4,5,6,7,8$	$6/5$

Table B.4 continued from previous page

Matroid	Port	Bound on $\lambda(\Gamma)$
280230	$0,1,2,3,4,5,6,7,8$	6/5
280241	$0,1,2,3,4,5,6,7,8$	6/5
280246	$0,1,2,3,4,5,6,7,8$	6/5
280249	$0,1,2,3,4,5,6,7,8$	6/5
280253	$0,1,2,3,4,5,6,7,8$	6/5
280254	$0,1,2,3,4,5,6,7,8$	6/5
280733	$0,1,2,3,4,5,6,7,8$	6/5
280891	$0,1,2,3,4,5,6,7,8$	6/5
281004	$0,1,2,3,4,5,6,7,8$	6/5
281568	$0,1,2,3,4,5,6,7,8$	6/5
281572	$0,1,2,3,4,5,6,7,8$	6/5
281581	$0,1,2,3,4,5,6,7,8$	6/5
281794	$0,1,2,3,4,5,6,7,8$	6/5
282270	$0,1,2,3,4,5,6,7,8$	6/5
282271	$0,1,2,3,4,5,6,7,8$	6/5
282272	$0,1,2,3,4,5,6,7,8$	6/5
283581	$0,1,2,3,4,5,6,7,8$	6/5
283624	$0,1,2,3,4,5,6,7,8$	6/5
283626	$0,1,2,3,4,5,6,7,8$	6/5
283630	$0,1,2,3,4,5,6,7,8$	6/5
283631	$0,1,2,3,4,5,6,7,8$	6/5
283632	$0,1,2,3,4,5,6,7,8$	6/5
291383	$0,1,2,3,4,5,6,7,8$	6/5
292609	$0,1,2,3,4,5,6,7,8$	6/5
293346	$0,1,2,3,4,5,6,7,8$	6/5
293347	$0,1,2,3,4,5,6,7,8$	6/5
293361	$0,1,2,3,4,5,6,7,8$	6/5
294990	$0,1,2,3,4,5,6,7,8$	6/5
295231	$0,1,2,3,4,5,6,7,8$	6/5
299715	$0,1,2,3,4,5,6,7,8$	6/5
299721	$0,1,2,3,4,5,6,7,8$	6/5
300609	$0,1,2,3,4,5,6,7,8$	6/5
300831	$0,1,2,3,4,5,6,7,8$	6/5
301018	$0,1,2,3,4,5,6,7,8$	6/5
303086	$0,1,2,3,4,5,6,7,8$	6/5
303094	$0,1,2,3,4,5,6,7,8$	6/5
303095	$0,1,2,3,4,5,6,7,8$	6/5
303158	$0,1,2,3,4,5,6,7,8$	6/5
303165	$0,1,2,3,4,5,6,7,8$	6/5
303175	$0,1,2,3,4,5,6,7,8$	6/5
304062	$0,1,2,3,4,5,6,7,8$	6/5
304066	$0,1,2,3,4,5,6,7,8$	6/5
304067	$0,1,2,3,4,5,6,7,8$	6/5
304085	$0,1,2,3,4,5,6,7,8$	6/5
306452	$0,1,2,3,4,5,6,7,8$	6/5
308279	$0,1,2,3,4,5,6,7,8$	6/5
308280	$0,1,2,3,4,5,6,7,8$	6/5

Table B.4 continued from previous page

Matroid	Port	Bound on $\lambda(\Gamma)$
308285	$0,1,2,3,4,5,6,7,8$	6/5
308381	$0,1,2,3,4,5,6,7,8$	6/5
308385	$0,1,2,3,4,5,6,7,8$	6/5
308386	$0,1,2,3,4,5,6,7,8$	6/5
319504	$0,1,2,3,4,5,6,7,8$	6/5
320838	$0,1,2,3,4,5,6,7,8$	6/5
327043	$0,1,2,3,4,5,6,7,8$	6/5
327134	$0,1,2,3,4,5,6,7,8$	6/5
327157	$0,1,2,3,4,5,6,7,8$	6/5
328810	$0,1,2,3,4,5,6,7,8$	6/5
328817	$0,1,2,3,4,5,6,7,8$	6/5
328818	$0,1,2,3,4,5,6,7,8$	6/5
328917	$0,1,2,3,4,5,6,7,8$	6/5
328928	$0,1,2,3,4,5,6,7,8$	6/5
328941	$0,1,2,3,4,5,6,7,8$	6/5
335557	$0,1,2,3,4,5,6,7,8$	6/5
335558	$0,1,2,3,4,5,6,7,8$	6/5
350495	$0,1,2,3,4,5,6,7,8$	6/5
351377	$0,1,2,3,4,5,6,7,8$	6/5
351471	$0,1,2,3,4,5,6,7,8$	6/5
351483	$0,1,2,3,4,5,6,7,8$	6/5
Tic-Tac-Toe	$0,1,2,3,4,5,6,7,8$	6/5

TABLE B.4: Bounds on $\lambda(\Gamma)$ for all Ingleton-Compliant Non-GP (5,9) Matroids

B.4 Proof of Lower Bound on λ for a Port of Vámos Matroid

The Vámos matroid is a sparse paving $(4,8)$ matroid. Its circuit-hyperplanes are the 4-sets 0123, 0145, 0167, 2345 and 4567. Martí-Farré and Padró [78] showed that for any port Γ of this matroid, $\lambda(\Gamma) \leq 4/3$. Farràs et al. [50] proved that this was optimal by showing that $\lambda(\Gamma) \geq 4/3$. This lower bound was obtained computationally using the CI technique. In this section we show a manually verifiable proof of the result.

The Vámos matroid has two ports, up to isomorphism. The port at 1 has the following minimal authorized sets

$$\min \Gamma_1 = \{023, 045, 067\} \cup \{A \in \binom{8}{4} : A \text{ is not a circuit-hyperplane}\}.$$

The ports at 0, 4, and 5 are all isomorphic to this access structure, while the ports at 2, 3, 6, and 7 are all isomorphic to each other.

Theorem B.1. *For the access structure Γ_1 of the Vámos matroid, $\lambda(\Gamma_1) = 4/3$.*

Proof. The upper bound was proved in [78], so we skip it.

To prove the lower bound, we first apply the same approach as [50] by solving the linear programming problem. The set up for this LP problem is as follows. The secret is 0 (though we're dealing with the port at 1, in our programs we relabel this point by 0 for simplification), the participants are $\{1, 2, 3, 4, 5, 6, 7\}$ and we take the common information $8 = CI(45, 67)$ to obtain a final ground set $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$. We then run this LP with objective function $\lambda(\Gamma_1)$ and constraints derived from the polymatroid and CI axioms.

Following this, we look at the solution of this LP problem to obtain the dual value of each constraint in the problem. For each constraint, this value serves as a coefficient of each of its terms in the solution. The constraints with a non-zero dual value are given below.

$$
\begin{array}{rrr}
2(\lambda(\Gamma_1) - f(1)) \geq 0 & f(6:8|0237) \geq 0 & f(4:6|02378) \geq 0 \\
\lambda(\Gamma_1) - f(6) \geq 0 & f(2:8|0147) \geq 0 & f(5:6|23478) \geq 0 \\
f(\emptyset) = 0 & f(3:8|01247) \geq 0 & f(1:6|234578) \geq 0 \\
2f(1|02345678) \geq 0 & f(0:8|2347) \geq 0 & f(0:4|678) \geq 0 \\
f(6|01234578) \geq 0 & f(6:8|012347) \geq 0 & f(1:4|0678) \geq 0 \\
7f(8|01234567) \geq 0 & f(6:8|0123457) \geq 0 & f(0:5|4678) \geq 0 \\
f(4:8) \geq 0 & f(4:8|2367) \geq 0 & f(1:2|04678) \geq 0 \\
f(5:8) \geq 0 & f(1:8|023467) \geq 0 & f(1:5|024678) \geq 0 \\
f(6:8) \geq 0 & f(5:8|0123467) \geq 0 & f(1:3|245678) \geq 0 \\
f(6:7|1) \geq 0 & f(4:8|0123567) \geq 0 & f(0:1|2345678) \geq 0 \\
f(6:8|01) \geq 0 & f(2:8|04567) \geq 0 & -1(f(0|1) = 1) \\
f(4:8|23) \geq 0 & f(1:8|24567) \geq 0 & -f(0|123) = 0 \\
f(7:8|23) \geq 0 & 2f(3:8|0124567) \geq 0 & f(0|14) = 1 \\
f(6:8|123) \geq 0 & f(0:8|1234567) \geq 0 & -f(0|145) = 0 \\
f(1:5|4) \geq 0 & f(1:2|8) \geq 0 & f(0|2345) = 1 \\
f(5:8|014) \geq 0 & f(1:4|8) \geq 0 & -f(0|12345) = 0 \\
f(5:8|234) \geq 0 & f(1:6|8) \geq 0 & f(0|146) = 1 \\
f(6:8|5) \geq 0 & f(1:7|8) \geq 0 & -f(0|1246) = 0 \\
f(6:8|45) \geq 0 & f(0:4|18) \geq 0 & f(0|12346) = 0 \\
f(1:8|02345) \geq 0 & f(0:5|18) \geq 0 & f(0|156) = 1 \\
f(7:8|12345) \geq 0 & f(1:3|28) \geq 0 & f(0|237) = 1 \\
f(4:8|16) \geq 0 & f(0:6|148) \geq 0 & f(0|147) = 1 \\
f(7:8|016) \geq 0 & f(0:7|148) \geq 0 & -f(0|2347) = 0 \\
f(4:8|1236) \geq 0 & f(0:6|158) \geq 0 & f(0|123457) = 0 \\
f(2:8|0146) \geq 0 & f(0:2|458) \geq 0 & -f(0|167) = 0 \\
f(5:8|1246) \geq 0 & f(1:2|0458) \geq 0 & -f(0|2367) = 0 \\
f(7:8|012346) \geq 0 & f(1:3|2458) \geq 0 & f(0|23467) = 0 \\
f(1:8|56) \geq 0 & f(0:6|12458) \geq 0 & f(0|4567) = 1 \\
f(2:8|0156) \geq 0 & f(1:6|023458) \geq 0 & -f(0|24567) = 0 \\
f(3:8|01256) \geq 0 & f(0:3|12468) \geq 0 & 2f(0|124567) = 0 \\
f(7:8|012356) \geq 0 & f(0:7|124568) \geq 0 & -f(0|1234567) = 0 \\
f(7:8|456) \geq 0 & f(1:7|0234568) \geq 0 & -4f(8|01) = 0 \\
f(7:8|12456) \geq 0 & f(2:6|78) \geq 0 & -f(8|23) = 0 \\
f(4:8|17) \geq 0 & f(3:6|278) \geq 0 & -(f(8) = f(01:23))
\end{array}
$$

Summing these inequalities, they resolve into

$$3\lambda(\Gamma_1) \geq 2f(8|01234567) + 4 = 4.$$

This implies $\lambda(\Gamma_1) \geq 4/3$. □

B.5 Proof of Lower Bound on λ for a Port of Tic-Tac-Toe Matroid

The Tic-Tac-Toe matroid is a sparse paving $(5, 9)$ matroid with circuit-hyperplanes $\mathcal{C} = \{01236, 01247, 01258, 03456, 23458, 03678, 14678, 25678\}$. In Section 5.4, we showed that $\lambda(\Gamma) = 6/5$ for at least one of the ports of the Tic-Tac-Toe matroid. The upper bound was proved using λ-decompositions, while the lower bound was obtained computationally using the CI property (see Appendix B.3). We present a manually verifiable proof of this lower bound here.

Up to isomorphism, there are only 3 ports for the Tic-Tac-Toe matroid. The port we consider in this section, which is the port at 6, is the access structure with minimal authorized sets

$$\min \Gamma_6 = \{0123, 0345, 0378, 1478, 2578\} \cup \{A \in \binom{9}{5} : A \notin \mathcal{C}\}.$$

Isomorphic to Γ_6 are the ports at 0, 2, and 8. Isomorphic to the port at 5 are the ports at 1, 3, and 7. The port at 4 stands alone.

Theorem B.2. *For the access structure Γ_6 of the Tic-Tac-Toe matroid, $\lambda(\Gamma_6) = 6/5$.*

Proof. The upper bound was proved in Section 5.4, so we deal with the lower bound here.

The approach we follow here is similar to that of Theorem B.1. The ground set is given as $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ where $9 = CI(258, 036)$ and 0 is the relabelled secret.

From the solution of this problem we obtain the dual value for the constraints, and those with a value different from zero are presented below. Those with a minus sign have a dual value -1 while those without any preceding number have a dual value of 1. The rest have as dual value the number that precedes them.

$$\lambda(\Gamma_6) - f(1) \geq 0$$
$$\lambda(\Gamma_6) - f(3) \geq 0$$
$$\lambda(\Gamma_6) - f(6) \geq 0$$
$$\lambda(\Gamma_6) - f(7) \geq 0$$
$$\lambda(\Gamma_6) - f(8) \geq 0$$
$$3f(\emptyset) = 0$$
$$2(f(0) = 1)$$
$$3f(0|123456789) \geq 0$$
$$f(1|023456789) \geq 0$$
$$f(3|012456789) \geq 0$$
$$f(6|012345789) \geq 0$$
$$f(7|012345689) \geq 0$$
$$f(8|012345679) \geq 0$$
$$8f(9|012345678) \geq 0$$
$$f(1:3) \geq 0$$
$$f(2:7) \geq 0$$
$$f(8:9) \geq 0$$
$$f(1:7|0) \geq 0$$
$$f(3:6|0) \geq 0$$
$$f(3:6|01) \geq 0$$
$$f(5:7|2) \geq 0$$
$$f(4:6|3) \geq 0$$
$$f(5:6|34) \geq 0$$
$$f(7:8|25) \geq 0$$
$$f(7:9|345) \geq 0$$
$$f(0:9|6) \geq 0$$
$$f(2:3|16) \geq 0$$
$$f(7:9|126) \geq 0$$
$$2f(1:9|36) \geq 0$$
$$f(7:8|36) \geq 0$$
$$f(8:9|36) \geq 0$$
$$f(5:9|036) \geq 0$$
$$f(8:9|136) \geq 0$$
$$f(2:9|0136) \geq 0$$
$$f(4:9|0356) \geq 0$$
$$f(0:9|12456) \geq 0$$
$$f(1:4|07) \geq 0$$
$$f(1:8|47) \geq 0$$
$$f(0:9|12347) \geq 0$$
$$f(0:9|12457) \geq 0$$
$$f(1:8|03457) \geq 0$$
$$f(2:9|13457) \geq 0$$
$$f(6:8|123457) \geq 0$$
$$f(4:9|1267) \geq 0$$
$$f(5:9|367) \geq 0$$
$$f(5:9|012467) \geq 0$$
$$f(4:9|03567) \geq 0$$
$$f(8:9|0124567) \geq 0$$
$$f(1:9|34567) \geq 0$$
$$f(2:9|134567) \geq 0$$
$$2f(8:9|01234567) \geq 0$$
$$2f(0:9|28) \geq 0$$
$$f(1:9|258) \geq 0$$
$$f(3:9|258) \geq 0$$
$$2f(6:9|258) \geq 0$$
$$f(7:9|0258) \geq 0$$
$$f(3:9|01258) \geq 0$$
$$f(4:9|2358) \geq 0$$
$$f(7:9|12358) \geq 0$$
$$f(1:9|023458) \geq 0$$
$$f(7:9|123458) \geq 0$$
$$2f(7:9|0368) \geq 0$$
$$f(4:9|01368) \geq 0$$
$$f(7:9|13468) \geq 0$$
$$f(1:9|2568) \geq 0$$
$$f(4:9|02568) \geq 0$$
$$f(7:9|012568) \geq 0$$
$$f(1:7|23568) \geq 0$$
$$2f(4:9|23568) \geq 0$$
$$f(7:9|23568) \geq 0$$
$$f(4:7|0123568) \geq 0$$
$$f(1:9|24568) \geq 0$$
$$f(7:9|0124568) \geq 0$$
$$f(1:9|234568) \geq 0$$
$$f(1:9|0234568) \geq 0$$
$$3f(7:9|01234568) \geq 0$$
$$f(1:9|0478) \geq 0$$
$$f(0:9|13578) \geq 0$$
$$f(6:9|123578) \geq 0$$
$$f(1:9|34578) \geq 0$$
$$2f(6:9|01234578) \geq 0$$
$$f(4:9|3678) \geq 0$$
$$f(5:9|34678) \geq 0$$
$$f(2:9|134678) \geq 0$$
$$f(5:9|01234678) \geq 0$$
$$f(4:9|0125678) \geq 0$$
$$2f(4:9|0235678) \geq 0$$
$$f(4:9|01235678) \geq 0$$
$$3f(3:9|01245678) \geq 0$$
$$f(1:2|345678) \geq 0$$
$$f(2:9|01345678) \geq 0$$
$$3f(1:9|02345678) \geq 0$$
$$f(0:1|9) \geq 0$$
$$f(0:7|9) \geq 0$$
$$3f(3:8|9) \geq 0$$
$$f(3:7|09) \geq 0$$
$$f(6:8|09) \geq 0$$
$$f(0:5|19) \geq 0$$
$$3f(0:8|39) \geq 0$$
$$f(6:7|039) \geq 0$$
$$3f(6:8|039) \geq 0$$
$$f(0:8|159) \geq 0$$
$$f(0:2|3459) \geq 0$$
$$f(6:7|03459) \geq 0$$
$$f(0:8|23459) \geq 0$$
$$f(3:8|69) \geq 0$$
$$f(0:5|1269) \geq 0$$
$$f(3:5|01269) \geq 0$$
$$f(0:1|369) \geq 0$$
$$2f(0:4|369) \geq 0$$
$$f(0:5|369) \geq 0$$
$$2f(0:2|3469) \geq 0$$
$$2f(0:1|23469) \geq 0$$
$$2f(0:7|123469) \geq 0$$
$$f(0:8|12569) \geq 0$$
$$f(3:4|012569) \geq 0$$
$$f(0:7|3569) \geq 0$$

$$
\begin{array}{rrr}
f(3:8|124569) \geq 0 & f(0:5|134689) \geq 0 & 2f(0|1234567) = 0 \\
f(0:7|1234569) \geq 0 & f(0:7|1235689) \geq 0 & -2(f(0|28) = 1) \\
f(4:8|79) \geq 0 & f(0:3|245689) \geq 0 & f(0|258) = 1 \\
f(1:5|479) \geq 0 & f(3:7|01245689) \geq 0 & f(0|1258) = 1 \\
f(0:6|1479) \geq 0 & f(0:2|1345689) \geq 0 & -f(0|12358) = 0 \\
f(3:8|01479) \geq 0 & f(0:4|789) \geq 0 & f(0|23458) = 1 \\
f(2:8|013479) \geq 0 & f(5:6|0789) \geq 0 & -f(0|123458) = 0 \\
f(6:8|123479) \geq 0 & f(0:6|1234789) \geq 0 & 2(f(0|368) = 1) \\
f(1:3|4579) \geq 0 & f(2:6|05789) \geq 0 & f(0|1368) = 1 \\
f(0:3|124579) \geq 0 & f(0:4|135789) \geq 0 & -f(0|13468) = 0 \\
f(1:6|034579) \geq 0 & f(1:6|345789) \geq 0 & f(0|2568) = 1 \\
f(2:6|0134579) \geq 0 & f(0:2|1345789) \geq 0 & f(0|12568) = 1 \\
f(0:1|3679) \geq 0 & f(3:5|06789) \geq 0 & -4f(0|23568) = 0 \\
f(0:5|13679) \geq 0 & f(0:5|36789) \geq 0 & f(0|123568) = 0 \\
f(0:2|14679) \geq 0 & f(2:3|056789) \geq 0 & -f(0|24568) = 0 \\
2f(0:5|1234679) \geq 0 & f(0:2|356789) \geq 0 & f(0|124568) = 0 \\
f(5:8|1234679) \geq 0 & -(f(0|3) = 1) & f(0|234568) = 0 \\
f(0:2|135679) \geq 0 & -(f(0|13) = 1) & f(0|1234568) = 0 \\
f(0:4|1235679) \geq 0 & -2(f(0|6) = 1) & f(0|478) = 1 \\
f(0:1|345679) \geq 0 & -(f(0|16) = 1) & -f(0|1478) = 0 \\
f(0:8|1345679) \geq 0 & -3(f(0|36) = 1) & -f(0|2578) = 0 \\
4f(0:8|12345679) \geq 0 & 2(f(0|136) = 1) & -f(0|13578) = 0 \\
2f(2:6|89) \geq 0 & -f(0|1236) = 0 & -f(0|34578) = 0 \\
f(5:6|089) \geq 0 & -f(0|12456) = 0 & f(0|134578) = 0 \\
2f(0:5|289) \geq 0 & -f(0|3456) = 0 & 2f(0|1234578) = 0 \\
2f(3:5|289) \geq 0 & -(f(0|47) = 1) & -2f(0|3678) = 0 \\
2f(5:6|2389) \geq 0 & f(0|147) = 1 & f(0|1234678) = 0 \\
f(2:6|0589) \geq 0 & -f(0|12347) = 0 & 2f(0|235678) = 0 \\
f(0:2|1589) \geq 0 & -f(0|12457) = 0 & f(0|1345678) = 0 \\
f(0:6|123589) \geq 0 & f(0|3457) = 1 & f(0|2345678) = 0 \\
f(0:6|1234589) \geq 0 & -f(0|13457) = 0 & -2f(0|12345678) = 0 \\
3f(2:3|689) \geq 0 & f(0|12467) = 1 & -8f(9|258) = 0 \\
f(3:5|2689) \geq 0 & f(0|3567) = 1 & -9f(9|036) = 0 \\
f(0:1|3689) \geq 0 & -f(0|34567) = 0 & -4(f(9) = f(036:258))
\end{array}
$$

Summing these equalities and inequalities, we get

$$5\lambda(\Gamma_6) \geq 2 + 5f(9|012345678) + 4 = 6.$$

Hence, $\lambda(\Gamma_6) \geq 6/5$ as desired. □

UNIVERSITAT ROVIRA I VIRGILI
COMMON INFORMATION TECHNIQUES FOR THE STUDY OF MATROID REPRESENTATION AND SECRET SHARING SCHEMES
Michael Olugbenga Bamiloshin

Bibliography

[1] R. Ahlswede and J. Körner. On the connection between the entropies of input and output distributions of discrete memoryless channels. In *Proceedings of the 5th Brasov Conference on Probability Theory, Brasov, 1974.*, pages 13—23. Editura Academiei, Bucuresti, 1977.

[2] R. Ahlswede and J. Körner. On common information and related characteristics of correlated information sources. In *General Theory of Information Transfer and Combinatorics.*, pages 664–677. Springer, Berlin, Heidelberg, 2006.

[3] M. Alfter and W. Hochstättler. On pseudomodular matroids and adjoints. *Discrete Applied Mathematics*, 60:3–11, 1995.

[4] B. Applebaum and B. Arkis. On the power of amortization in secret sharing: d-uniform secret sharing and CDS with constant information rate. In *Theory of Cryptography Conference*, pages 317–344. Springer, 2018.

[5] B. Applebaum, A. Beimel, O. Farràs, O. Nir, and N. Peter. Secret-sharing schemes for general and uniform access structures. In *Advances in Cryptology - EUROCRYPT 2019*, volume 11478 of *Lecture Notes in Computer Science*, pages 441–471. Springer, 2019.

[6] B. Applebaum, A. Beimel, O. Nir, and N. Peter. Better secret sharing via robust conditional disclosure of secrets. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pages 280–293, 2020.

[7] L. Babai, A. Gál, and A. Wigderson. Superpolynomial lower bounds for monotone span programs. *Combinatorica*, 19:301–319, 1999.

[8] A. Bachem and W. Kern. On sticky matroids. *Discrete mathematics*, 69(1):11–18, 1988.

[9] A. Bachem and A. Wanka. Euclidean intersection properties. *Journal of Combinatorial Theory, Series B*, 47(1):10–19, 1989.

[10] M. Bamiloshin, A. Ben-Efraim, O. Farràs, and C. Padró. Common information, matroid representation, and secret sharing for matroid ports. *Designs, Codes, and Cryptography*, 89:143–166, 2021.

[11] N. Bansal, R. A. Pendavingh, and J. G. van der Pol. On the number of matroids. *Combinatorica*, 35(3):253–277, 2015.

[12] A. Beimel. Secure schemes for secret sharing and key distribution. 1996. PhD thesis.

[13] A. Beimel. Secret-sharing schemes: A survey. In *International conference on coding and cryptology*, pages 11–46. Springer, 2011.

[14] A. Beimel, A. Ben-Efraim, C. Padró, and I. Tyomkin. Multi-linear secret-sharing schemes. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) LNAI*, 8349:394–418, 2014.

[15] A. Beimel and O. Farràs. The share size of secret-sharing schemes for almost all access structures and graphs. In *Theory of Cryptography Conference*, pages 499–529. Springer, 2020.

[16] A. Beimel, A. Gál, and M. Paterson. Lower bounds for monotone span programs. *Comput. Complexity*, 6:29–45, 1997.

[17] A. Beimel and N. Livne. On matroids and nonideal secret sharing. *In* IEEE Transactions on Information Theory, 54(6):2626–2643, 2008.

[18] A. Beimel, N. Livne, and C. Padró. Matroids can be far from ideal secret sharing. *Fifth Theory of Cryptography Conference, TCC 2008, Lecture Notes in Comput. Sci*, 4948:194–212, 2008.

[19] A. Beimel and I. Orlov. Secret sharing and non-Shannon information inequalities. *IEEE Trans Inform. Theory*, 57:5634–5649, 2011.

[20] A. Beimel and N. Peter. Optimal linear multiparty conditional disclosure of secrets protocols. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 332–362. Springer, 2018.

[21] A. Beimel, T. Tassa, and E. Weinreb. Characterizing ideal weighted threshold secret sharing. In *Theory of Cryptography Conference*, pages 600–619. Springer, 2005.

[22] A. Ben-Efraim. Secret-sharing matroids need not be algebraic. *Discrete Mathematics*, 339(8):2136–2145, 2016.

[23] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, pages 1–10, New York, NY, USA, 1988. Association for Computing Machinery.

[24] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. *Advances in Cryptology—CRYPTO'88, Lecture Notes in Comput. Sci*, 403:27–35, 1990.

[25] M. Bertilsson and I. Ingemarsson. A construction of practical secret sharing schemes using linear block codes. In *Advances in Cryptology - AUSCRYPT '92*, volume 718, pages 67–79, 1992.

[26] G. R. Blakley. Safeguarding cryptographic keys. In *Managing Requirements Knowledge, International Workshop on*, page 313. IEEE Computer Society, 1979.

[27] G. P. Bollen. `https://github.com/gpbollen/Algebraicity-of-Matroids-and-Frobenius-Flocks`.

[28] G. P. Bollen. Frobenius flocks and algebraicity of matroids. *Technische Universiteit Eindhoven*, 2018. PhD Thesis.

[29] G. P. Bollen, D. Cartwright, and J. Draisma. Matroids over one-dimensional groups. *International Mathematics Research Notices*, 2018.

[30] E. F. Brickell. Some ideal secret sharing schemes. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 468–475. Springer, 1989.

[31] E. F. Brickell and D. M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptology*, 4:123–134, 1991.

[32] A. Cameron. Kinser inequalities and related matroids. *arXiv preprint arXiv:1401.0500*, 2014.

[33] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro. On the size of shares for secret sharing schemes. *J. Cryptology*, 6:157–167, 1993.

[34] D. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditionally secure protocols. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, pages 11–19, New York, NY, USA, 1988. Association for Computing Machinery.

[35] R. Cramer, I. B. Damgård, and J. B. Nielsen. *Secure Multiparty Computation and Secret Sharing*. Cambridge University Press, USA, 1st edition, 2015.

[36] L. Csirmaz. The size of a share must be large. *J. Cryptology*, 10:223–231, 1997.

[37] L. Csirmaz. Secret sharing and duality. *Journal of Mathematical Cryptology*, 15(1):157–173, 2020.

[38] L. Csirmaz and P. Ligeti. LP problems in secret sharing. In *7th Hungarian-Japanese Symposium on Discrete Mathematics and Its Applications*, 2013.

[39] I. Csiszar and J. Körner. *Information theory: coding theorems for discrete memoryless systems*. Academic Press ; Akademiai Kiado, New York: Budapest, 1981.

[40] P. Dembowski. *Finite geometries*, volume 44. Springer Science & Business Media, 1968.

[41] R. Dougherty, C. Freiling, and K. Zeger. Six new non-Shannon information inequalities. In *2006 IEEE International Symposium on Information Theory*, pages 233–236, 2006.

[42] R. Dougherty, C. Freiling, and K. Zeger. Networks, matroids, and non-Shannon information inequalities. *IEEE Trans. Inform. Theory*, 53(6):1949–1969, 2007.

[43] R. Dougherty, C. Freiling, and K. Zeger. Linear rank inequalities on five or more variables. *Available at arXiv.org*, 2009.

[44] R. Dougherty, C. Freiling, and K. Zeger. Non-Shannon information inequalities in four random variables. *Available at arXiv.org*, 2011.

[45] R. Dougherty, C. Freiling, and K. Zeger. Characteristic-dependent linear rank inequalities with applications to network coding. *IEEE Trans. Inform. Theory*, 5(61):2510–2530, 2015.

[46] A. Dress and L. Lovasz. On some combinatorial properties of algebraic matroids. *Combinatorica*, 7(1):39–48, 1987.

[47] O. Farràs. Secret sharing schemes for ports of matroids of rank 3. *Kybernetika*, 56(5):903–915, 2020.

[48] O. Farràs, T. Hansen, T. Kaced, and C. Padró. On the information ratio of non-perfect secret sharing schemes. *Algorithmica*, 79(4):987–1013, 2017.

[49] O. Farràs, T. Kaced, S. Martín, and C. Padró. Improving the linear programming technique in the search for lower bounds in secret sharing. *Advances in Cryptology — Eurocrypt 2018, Lecture Notes in Comput. Sci.*, 10820:597–621, 2018. Full version is available at Cryptology ePrint Archive, Report 2017/919.

[50] O. Farràs, T. Kaced, S. Martín, and C. Padró. Improving the linear programming technique in the search for lower bounds in secret sharing. *IEEE Transactions on Information Theory*, 2020. Full version of [49].

[51] O. Farràs, J. Martí-Farré, and C. Padró. Ideal multipartite secret sharing schemes. *Journal of cryptology*, 25(3):434–463, 2012.

[52] O. Farras and C. Padró. Ideal hierarchical secret sharing schemes. *IEEE transactions on information theory*, 58(5):3273–3286, 2012.

[53] O. Farràs, J. Ribes-González, and S. Ricci. Local bounds for the optimal information ratio of secret sharing schemes. *Designs, Codes and Cryptography*, 87(6):1323–1344, 2019.

[54] S. Fujishige. Entropy functions and polymatroids—combinatorial structures in information theory. *Electron. Comm. Japan*, 61:14–18, 1978.

[55] S. Fujishige. Polymatroidal dependence structure of a set of random variables. *Information and Control*, 39:55–72, 1978.

[56] P. Gács and J. Körner. Common information is far less than mutual information. *Problems of Contr. and Inf. Th.*, 2:149–162, 1973.

[57] L. Guillé, T. Chan, and A. Grant. The minimal set of Ingleton inequalities. *IEEE transactions on information theory*, 57(4):1849–1864, 2011.

[58] E. Gürpinar and A. Romashchenko. How to use undiscovered information inequalities: Direct applications of the copy lemma. In *IEEE International Symposium on Information Theory, ISIT 2019, Paris, France, July 7-12, 2019*, pages 1377–1381. IEEE, 2019.

[59] D. Hammer, A. E. Romashchenko, A. Shen, and N. K. Vereshchagin. Inequalities for Shannon entropy and Kolmogorov complexity. *Journal of Computer and Systems Sciences*, 60:442–464, 2000.

[60] W. Hochstättler. About the tic-tac-toe matroid. *Technical Report. Universität zu Köln, Angewandte Mathematik und Informatik*, (97.272), 1997.

[61] A. W. Ingleton. Representation of matroids. In D. J. A. Welsh, editor, *Combinatorial Mathematics and its Applications*, pages 149–167. Academic Press, London, 1971.

[62] A. W. Ingleton and R. A. Main. Non-algebraic matroids exist. *Bull London Math Soc.*, 7:144–146, 1975.

[63] M. Ito, A. Saito, and T. Nishizeki. Secret sharing scheme realizing any access structure. In *Proc. IEEE Globecom'87*, pages 99–102, 1987.

[64] W. A. Jackson and K. M. Martin. Geometric secret sharing schemes and their duals. *Des. Codes Cryptogr.*, 4:83–95, 1994.

[65] W. A. Jackson and K. M. Martin. Perfect secret sharing schemes on five participants. *Des. Codes Cryptogr.*, 9:267–286, 1996.

[66] T. Kaced. Equivalence of two proof techniques for non-Shannon inequalities. In *2013 IEEE International Symposium on Information Theory*, pages 236–240, 2013.

[67] T. Kaced. Information inequalities are not closed under polymatroid duality. *IEEE Trans. Inform. Theory*, 64:4379–4381, 2018.

[68] M. Karchmer and A. Wigderson. On span programs. In *Proc. of the 8th IEEE Structure in Complexity Theory*, pages 102–111, 1993.

[69] E. D. Karnin, J. W. Greene, and M. E. Hellman. On secret sharing systems. *IEEE Trans. Inform. Theory*, 29:35–41, 1983.

[70] R. Kinser. New inequalities for subspace arrangements. *J. Combin. Theory Ser. A*, 118:152–161, 2011.

[71] A. Lehman. A solution of the Shannon switching game. *Journal of the Society for Industrial and Applied Mathematics*, 12(4):687–725, 1964.

[72] B. Lindström. A non-linear algebraic matroid with infinite characteristic set. *Discrete Mathematics*, 59:319–320, 1986.

[73] B. Lindström. A class of non-algebraic matroids of rank three. *Geometriae Dedicata*, 23(3):255–258, 1987.

[74] B. Lindström. A generalization of the Ingleton-Main lemma and a class of non-algebraic matroids. *Combinatorica*, 8(1):87–90, 1988.

[75] T. Liu and V. Vaikuntanathan. Breaking the circuit-size barrier in secret sharing. In *50th STOC 2018*, pages 699–708, 2018.

[76] T. Liu, V. Vaikuntanathan, and H. Wee. Conditional disclosure of secrets via non-linear reconstruction. In *Annual International Cryptology Conference*, pages 758–790. Springer, 2017.

[77] K. Makarychev, Y. Makarychev, A. Romashchenko, and N. Vereshchagin. A new class of non-Shannon-type inequalities for entropies. *Communications in Information and Systems*, 2:147–166, 2002.

[78] J. Martí-Farré and C. Padró. On secret sharing schemes, matroids and polymatroids. *J. Math. Cryptol.*, 4:95–120, 2010.

[79] S. Martín, C. Padró, and A. Yang. Secret sharing, rank inequalities, and information inequalities. *IEEE Trans. Inform. Theory*, 62:599–609, 2016.

[80] F. Matúš. Matroid representations by partitions. *Discrete Mathematics*, 203:169–194, 1999.

[81] F. Matúš. Infinitely many information inequalities. In *Proc. IEEE International Symposium on Information Theory, (ISIT)*, pages 2101–2105, 2007.

[82] F. Matúš. Algebraic matroids are almost entropic. 2017. To appear in Proceedings of the AMS.

[83] F. Matúš. Classes of matroids closed under minors and principal extensions. *Combinatorica*, 38:935–954, 2018.

[84] F. Matúš and L. Csirmaz. Entropy region and convolution. *IEEE Trans. Inform. Theory*, 62:6007–6018, 2016.

[85] D. Mayhew, M. Newman, D. Welsh, and G. Whittle. On the asymptotic proportion of connected matroids. *European Journal of Combinatorics*, 32(6):882 – 890, 2011.

[86] D. Mayhew, M. Newman, and G. Whittle. On excluded minors for real representability. *J. Comb. Th. B*, 99:685–689, 2009.

[87] D. Mayhew and G. F. Royle. Matroids with nine elements. *J. Combin. Theory Ser. B*, 98:415–431, 2008.

[88] D. Mayhew and D. Welsh. On the number of sparse paving matroids. *Advances in Applied Mathematics*, 50(1):125–131, 2013.

[89] J. R. Metcalf-Burton. Improved upper bounds for the information rates of the secret sharing schemes induced by the Vámos matroid. *Discrete Math.*, 311:651–662, 2011.

[90] P. Nelson and J. van der Pol. Doubly exponentially many Ingleton matroids. *SIAM Journal on Discrete Mathematics*, 32(2):1145–1153, 2018.

[91] J. G. Oxley. *Matroid theory*. Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, second edition, 2011.

[92] C. Padró. Lecture notes in secret sharing. *Cryptology ePrint Archive, Report 2012/674*, 2012.

[93] C. Padró, L. Vázquez, and A. Yang. Finding lower bounds on the complexity of secret sharing schemes by linear programming. *Discrete Applied Mathematics*, 161:1072–1084, 2013.

[94] V. Peña and H. Sarria. How to find new characteristic-dependent linear rank inequalities using binary matrices as a guide. 2019. Available at arXiv.org.

[95] R. Pendavingh and J. van der Pol. On the number of matroids compared to the number of sparse paving matroids. *arXiv preprint arXiv:1411.0935*, 2014.

[96] R. A. Pendavingh and S. H. M. van Zwam. Skew partial fields, multilinear representations of matroids, and a matrix tree theorem. *Adv. in Appl. Math*, 50:201–226, 2013.

[97] T. Pitassi and R. Robere. Lifting nullstellensatz to monotone span programs over any field. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, pages 1207–1219, 2018.

[98] R. Rado. Note on independence functions. In *Proc. London Math. Soc. (3) 7*, pages 300–320, 1957.

[99] G. Royle and D. Mayhew. Matroids on 9 elements. `http://doi.org/10.26182/5e3378f0ca2cd`.

[100] A. Schrijver. *Combinatorial optimization: Polyhedra and efficiency.* Springer-Verlag, Berlin, 2003.

[101] P. D. Seymour. On secret-sharing matroids. *J. Combin. Theory Ser. B*, 56:69–73, 1992.

[102] A. Shamir. How to share a secret. *Commun. of the ACM*, 22:612–613, 1979.

[103] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27(3):379–423, July 1948.

[104] J. Simonis and A. Ashikhmin. Almost affine codes. *Designs, Codes, and Cryptography*, 14(2):179–197, 1998.

[105] D. R. Stinson. Decomposition constructions for secret-sharing schemes. *IEEE Trans. Inform. Theory*, 40:118–125, 1994.

[106] S. Thakor, T. Chan, and A. Grant. Capacity bounds for networks with correlated sources and characterisation of distributions by entropies. *IEEE Trans. Inform. Theory*, 63:3540–3553, 2017.

[107] B. L. van der Waerden. *Moderne Algebra.* Springer, Berlin, 2nd edition, 1937.

[108] M. van Dijk. On the information rate of perfect secret sharing schemes. *Des. Codes Cryptogr.*, 6:143–169, 1995.

[109] D. Vertigan. Dowling geometries representable over rings. *Annals of Combinatorics*, 19, 2015.

[110] H. Whitney. On the abstract properties of linear dependence. *Amer. J. Math.*, 57:509–533, 1935.

[111] R. W. Yeung. *Information theory and network coding.* Springer, 2008.

[112] R. W. Yeung. *A first course in information theory.* Springer Science & Business Media, 2012.

[113] Z. Zhang and R. W. Yeung. A non-Shannon-type conditional inequality of information quantities. *IEEE Trans. Information Theory*, 43:1982–1986, 1997.

[114] Z. Zhang and R. W. Yeung. On characterization of entropy function via information inequalities. *IEEE Trans. Inform. Theory*, 44:1440–1452, 1998.

UNIVERSITAT
ROVIRA i VIRGILI