UNIVERSIDAD NACIONAL DE COLOMBIA

New Characteristic Dependent Linear Rank Inequalities

Victor Bryallan Peña Macias

Universidad Nacional de Colombia
Facultad de Ciencias
Departamento de Matemáticas
Bogotá, Colombia

2020

New Characteristic Dependent Linear Rank Inequalities

Victor Bryallan Peña Macias

Dissertation submitted to the Department of Mathematics in partial fulfilment of the requirements for the degrees of Doctor in Mathematics

Advisor
Dr. Humberto Sarria Zapata

Research Topic: Information Theory
Research Group: Teoría de Matrices

Universidad Nacional de Colombia
Facultad de Ciencias
Departamento de Matemáticas
Bogotá, Colombia

2020

"A mis padres Victor y Maria, mi esposa Kendy Johana, que siempre me han apoyado a lo largo de mi vida y mi carrera."

Acknowledgments

I would like to express my sincere gratitude to my advisor Humberto Sarria Zapata and La Universidad Nacional de Colombia for the knowledge provided. I also thank Carles Padró and La Universitat Politècnica de Catalunya for having me in my stay in Barcelona.

I deeply appreciate my wife and adventure partner Kendy Johana. Without her, all of this would not have been possible.

Finally I wish to thank COLCIENCIAS for the financial support.

Contents

List of Figures

Nomenclature

We write down the principal notation of this document. We have used letters for various concepts.

Symbols	Use
$A, B, C, ..., X, Y, W, Z, V...$	vector spaces or random variables
O	zero vector space
$\dim(A)$	dimension of a vector space A
$\mathrm{codim}_V(A)$	difference between the dimension of V and A
$\mathcal{A}$	alphabet
$\mathbb{F}$	finite field
$\mathrm{char}(\mathbb{F})$	characteristic of a field
f, g, ...	function, coding function
$\bar{f}$	partition
$\ker(f)$	partition into pre-images or kernel of a function f,
$\mathcal{F} = \left(\bar{f}_v\right)_{v \in V}$	family of partitions indexed by V
$\mathrm{H}(X)$	entropy
$\mathrm{H}(X \mid Y)$	conditional entropy
$\mathrm{I}(X;Y)$	mutual information
cl	closure operator
$\mathcal{M}$	matroid
r	rank of a matrix, matroid, closure operator
$\mathcal{B}_X^{\mathcal{M}}$	basis of X in a matroid $\mathcal{M}$
$\mathcal{M} \mid J$	matroid obtained by deletion of J
$[n]$	$\{1, \ldots, n\}$
$V + W$	sum of vector spaces
$V \oplus W$	direct sum of vector spaces
$[n, m]$, (n, m), $(n, m]$, $[n, m)$	interval notation with integer numbers

Symbols	Use
$\nabla(A_i : i \in X)$, $\Delta(A_i : i \in X)$	finite sums of entropies of A_i, $i \in X$
$\varphi(n, p)$	the function that counts all the powers of p less than or equal to n
e_i	vector with 1 in the i-component and 0 in otherwise
e_S	vector with 1 in the components indexed by S and 0 in otherwise
$[e_n]$, $\{e_i\}$	$\{e_1, \ldots, e_n\}$
$[e_n, e_m]$, (e_n, e_m), $(e_n, e_m]$, $[e_n, e_m)$	interval notation for set of vectors
B	it is also used to denote a binary matrix
$\mathcal{B}'$	in a binary matrix, the set $\{e_{S_i} : 1 < \lvert S_i\rvert < n\}$
$\mathcal{B}''$	in a binary matrix, the set $\{e_{S_i} : \lvert S_i\rvert = 1\}$
$\mathcal{B}'''$	$\{C\}$ or $\emptyset$
$\mathcal{B}_{e_i}$	in a binary matrix, the set $\left\{e_{S_j} : i \notin S_j\right\}$
$D = (V, E)$	digraph
$\mathcal{N} = (D, \tau)$	network
$\mathcal{N} = (D, S, T)$	multiple-unicast network
$\mathcal{N}_{\mathcal{M}} = (V, E^*_{\mathcal{M}})$	index-coding network from a matroid
b	optimal solution of a linear programming problem
B	inverse multiplicative of b
C	capacity of a network
$\mathrm{C}_{\mathrm{linear}}$	linear capacity of a network
$\mathrm{C}^{\mathcal{A}}_{D}(\mathrm{cl})$	capacity of a closure operator
$\sigma(\Sigma)$	information ratio of a secret sharing scheme
$\lambda(\Sigma)$	linear information ratio of a secret sharing scheme
$\sigma(\Gamma)$	information ratio of an access structure
$\lambda(\Gamma)$	linear information ratio of an access structure

Abstract

Abstract:

In this work, we develop some methods for producing characteristic-dependent linear rank inequalities and show some applications to Network Coding and Secrets Sharing. We propose two methods that take advantage of the existence of certain binary matrices. The first method is based on the construction of certain complementary vector spaces and has direct applications to Network Coding. Using linear programming problems, for each finite or co-finite set of primes P, we show as application that there exists a sequence of networks $(\mathcal{N}_t)$ in which each member is linearly solvable over a finite field if and only if the characteristic of the field is in P; and the linear capacity over fields whose characteristic is not in P, $\to 0$ as $t \to \infty$. The second method is based on the construction of certain spaces that behave in a certain way as a linear secret sharing scheme and has direct applications in Secret Sharing; we calculate lower bounds on the linear information ratios of some access structures. Additionally, we propose an extension of the solubility problem of a closure operator. We study the capacity of a closure operator and a class of linear programming problems whose optimal solutions are upper bounds on this capacity; this problem is related to the calculation of capacities of multiple-unicast networks.

Keywords: linear rank inequality, matroid, network coding, secret sharing, index coding, complementary vector space, binary matrix.

Mathematics subject classification: 94A15, 94A60, 62B10, 94A17

Victor Bryallan Peña Macias
vbpenam@unal.edu.co

Resumen:

En este trabajo estudiamos como construir desigualdades rango lineales dependientes de la característica y sus aplicaciones a la Teoría de Codificación de Redes y a la Teoría de Repartición de Secretos en protocolos criptográficos. Proponemos dos métodos que aprovechan la existencia de ciertas matrices binarias. El primer método está basado en la construcción de ciertos espacios vectoriales complementarios y tiene aplicaciones directas a la Teoría de Codificación de Redes. Presentando así, entre las aplicaciones y usando problemas de programación lineal, que para cada conjunto finito o cofinito de números primos P, existe una sucesión de redes $(\mathcal{N}_t)$, en la cual cada miembro es soluble linealmente sobre un cuerpo finito si, y sólo si, la característica del cuerpo está en P; además, la capacidad lineal sobre cuerpos cuya característica no está en P, tiende a 0, cuando t tiende a infinito. El segundo método está basado en la construcción de ciertos espacios que se comportan en cierta forma como un esquema de repartición de secretos y tiene aplicaciones directas en la Teoría de Repartición de Secretos; calculamos cotas inferiores de radios de información lineal de algunas estructuras. Adicionalmente, proponemos una extensión del problema de solubilidad de un operador de clausura. Estudiamos la capacidad de un operador de clausura y una serie de problemas de programación lineal cuyas soluciones son cotas superiores sobre esta capacidad; este problema está relacionado al cálculo de capacidades de redes de uniemisión múltiple.

Palabras clave: desigualdad rango lineal, matroide, codificación de redes, repartición de secretos, codificación de índices, espacio vectorial complementario, matriz binaria.

Clasificación por temas según AMS: 94A15, 94A60, 62B10, 94A17

Introduction

In Linear Algebra over finite fields, a *linear rank inequality* is a linear inequality that is always satisfied by ranks (dimensions) of subspaces of a vector space over any field. *Information inequalities* are a sub-class of linear rank inequalities [45]. The *Ingleton inequality* is an example of a linear rank inequality which is not information inequality [22], other inequalities have been presented in [13, 24] among others. A *characteristic-dependent linear rank inequality* is like a linear rank inequality but this is always satisfied by vector spaces over fields of certain characteristic and does not in general hold over other characteristics [14]. In Information Theory, especially in network coding and secret sharing, all these inequalities are useful to calculate bounds of rates (capacities, ratios of information) that measure the efficiency of communication [1, 4, 11, 14, 12, 17, 26]. We are interested in linear rates of communication in these areas.

The linear rate or linear capacity of a network depends on the characteristic of the scalar field associated to the vector space of the network codes [12, 8, 14]. Therefore, when we study linear capacities over specific fields, characteristic-dependent linear rank inequalities are more useful than usual linear rank inequalities. The use of characteristic-dependent linear rank inequalities in secret sharing is to date unknown; but we do know that there exist access structures that show efficiency in linear secret sharing schemes according to the choice of the characteristic of the fields where the schemes are defined [23]. Some results in secret sharing use linear rank inequalities with techniques of linear programming [17, 26]; this indicates that this type of inequality can be useful.

Characteristic-dependent linear rank inequalities have been presented in [5, 10, 18]. Dougherty, Freiling and Zeger have produced these inequalities used as a guide the network flow of some matroidal networks to obtain restrictions over linear solubility; these restrictions imply the inequalities. This technique has produced many inequalities [10, 18]: for each finite or co-finite set of primes, it is produced an inequality that is only true over fields whose characteristic is in that set. Blasiak, Kleinberg and Lubetzky have produced two inequalities from the dependency relations of the Fano and non-Fano matroids [5]. We remark that the technique used by Dougherty is different from the technique used by Blasiak. So we ask ourselves, can new inequalities be obtained from other suitable representable matroids

or using other techniques? In this dissertation, we answer affirmatively and produce many inequalities.

Characteristic-dependent linear rank inequalities have been used to demonstrate, among other things, that for any finite or co-finite set of prime numbers, there are networks that are linearly solvable over fields whose characteristic is in that set; and they are not solvable over fields with other characteristic [18]. In [5], using these inequalities and techniques of linear programming, there exists a sequence of networks $(\mathcal{N}_t)$ in which each member is asymptotically solvable but is not linearly solvable; and the linear capacity tends to 0 as t tends to infinity. Other related results are in [10].

Contributions. In this dissertation, we propose two methods for producing characteristic-dependent linear rank inequalities. We show two theorems that establish how to build these inequalities according the existence of binary matrices whose rank or determinant change depending on the characteristic of the field where its entries are defined. Each method can produce two types of inequalities for each $n \geq 7$: $\left\lfloor \frac{n-1}{2} \right\rfloor - 2$ inequalities that are true over finite sets of primes and other $\left\lfloor \frac{n-1}{2} \right\rfloor - 2$ inequalities that are true over co-finite sets of primes. The two inequalities of Blasiak et al. can be obtained combining some information inequalities with the inequality obtained by the first method and the usual representation matrix of the Fano matroid. In the context of applying these inequalities, we help enrich the theory. For each finite or co-finite set of primes P, we show that there exists a sequence of networks $(\mathcal{N}_t)$ in which each member is linearly solvable over a field if and only if the characteristic of the field is in P; and the linear capacity, over fields whose characteristic is not in P, tends to 0 as t tends to infinity. The consequences of this result improve known results in [5, 18, 33]. The closure solvability problem of a closure operator is studied in [19, 20, 36]; this concept is associated to the research of solvable multiple-unicast networks and p-representable matroids (which are related to secret sharing [28, 43, 44]). We extend that problem to the notion of (k, n)-fractional solvability problem of a closure operator. This allows defining linear programming problems (adding inequalities) in order to study which is the best partition solution of a closure operator over specific alphabets or finite fields. Using multiple-unicast network coding, we give some examples in which the (k, n)-fractional solvability problem is interesting. By last, in secret sharing, we calculate lower bounds on the ratios of linear information over some fields of ports of some representable matroids.

Organization of the work. In Chapter 1, we introduce the basic concepts of Information Theory, Matroids, Network Coding and Secret Sharing that are necessary to understand this document. In Chapter 2, we show our first method for producing characteristic-dependent linear rank inequalities; some inequalities are produced and some properties are derived. In Chapter 3, we show our second method for producing characteristic-dependent linear rank

inequalities; some inequalities are produced and some properties are derived. In Chapter 4, we introduce the (k, n)-solvability problem of a closure operator; a linear programming problem associated to this and some examples of application are presented. Later, we introduce some concepts of Index Coding in the context of Network Coding; we study some properties of the linear programming problem associated to these instances. We show some results of application to network coding using some inequalities of the first method. By last, using linear programming problems in Secret Sharing, we show some applications of the second method. In Chapter 5, we give some conclusions and possible work for future research.

Publications and Presentations

Publications:

- Characteristic-Dependent Linear Rank Inequalities in 21 Variables, Revista Academia Colombiana de Ciencias Exactas, Físicas y Naturales, 43(169): 765-770, 2019.
- Linear Programming Problems in Network Coding and Closure Operators via Partitions, Revista Selecciones Matemáticas, Universidad Nacional de Trujillo, Lima-Perú, 6(2): 269-274, 2019.
- Characteristic-Dependent Linear Rank Inequalities via Complementary Vector Spaces, Journal of Information and Optimization Sciences, Taylor & Francis Online co-published with Taru Publications, DOI: 10.1080/02522667.2019.1668157, 2020.
- How to Find New Characteristic-Dependent Linear Rank Inequalities using Binary Matrices as a Guide, Pre-print, 2019.
- How to Find New Characteristic-Dependent Linear Rank Inequalities using Secret Sharing, Pre-print, 2020.

Presentations:

- Desigualdades Rango Lineales Dependientes de la Característica, UN Encuentro de Matemáticas, Universidad Nacional de Colombia, Bogotá, 2018.
- Construcción de Desigualdades Rango Lineales Dependientes de la Característica usando Matrices Binarias como una Guía, XXII Congreso Colombiano de Matemáticas, Universidad del Cauca, Popayán, 2019.
- Particiones: Una Conexión entre Operadores de Clausura y Redes de Información, IX Congreso Internacional de Matemática Aplicada y Computacional, Lima-Perú, 2019.
- Characteristic-Dependent Linear Rank Inequalities and Applications to Network Coding, MAK Crypto Seminar, Departament de Matemàtiques, Universitat Politècnica de Catalunya, Barcelona-España, 2019.

1 Basics

In this chapter, we introduce some subject of Information Theory and matroids in order to understand this thesis.

1.1 Topics in Information Theory

Definition 1.1.1. [49] An *alphabet* $\mathcal{A}$ is a finite set with at least two elements. Let X be a discrete random variable, and let p be the probability density function of X over $\mathcal{A}$. The *entropy* $\mathrm{H}(X)$ of a random variable X is defined by

$$\mathrm{H}(X) := -\sum_{x \in \mathcal{A}} \mathrm{p}(x) \log \mathrm{p}(x).$$

The *joint entropy* $\mathrm{H}(X_1, ..., X_n)$ of a set of random variables $X_1, ..., X_n$ is defined by

$$\mathrm{H}(X_1, ..., X_n) := -\sum_{x_1, ...x_n} \mathrm{p}(x_1, ...x_n) \log \mathrm{p}(x_1, ...x_n).$$

For random variables X and Y, the *conditional entropy* of X given Y is defined by

$$\mathrm{H}(X \mid Y) := \mathrm{H}(X, Y) - \mathrm{H}(Y).$$

The *mutual information* between X and Y is denoted by

$$\mathrm{I}(X; Y) := \mathrm{H}(X) - \mathrm{H}(X \mid Y),$$

and the *conditional mutual information* between X and Y given Z is denoted by

$$\mathrm{I}(X; Y \mid Z) := \mathrm{H}(X, Z) - \mathrm{H}(X \mid Y, Z).$$

Let A, B, A_1, ..., A_n be vector subspaces of a finite dimensional vector space V over a finite field $\mathbb{F}$. Let $\sum_{i \in I} A_i$ be the span of A_i, $i \in I$. There is a correspondence between inequalities satisfied by dimensions of spans of vector spaces and inequalities satisfied by

entropies of certain class of random variables induced by vector spaces [45, Theorem 2]. We explain that: let f be chosen uniformly at random from the set of linear functions from V to $\mathbb{F}$. For A_1, ..., A_n, it is defined the random variables

$$X_1 = f\mid_{A_1},$$

$$\vdots$$

$$X_n = f\mid_{A_n}.$$

For $I \subseteq [n] := \{1, \ldots, n\}$, we have

$$\mathrm{H}\left(X_i : i \in I\right) = (\log|\mathbb{F}|)\dim\left(\sum_{i\in I} A_i\right).$$

The random variables X_1, ..., X_n are called *linear random variables over* $\mathbb{F}$. For simplicity, we identify the entropy of linear random variables with the dimension of the associated subspaces, i.e.

$$\mathrm{H}\left(A_i : i \in I\right) := \dim\left(\sum_{i\in I} A_i\right).$$

With this notation, the *mutual information* of A and B is given by

$$\mathrm{I}\left(A; B\right) = \dim\left(A \cap B\right).$$

The *codimension of A in V* is given by

$$\mathrm{codim}_V\left(A\right) = \dim\left(V\right) - \dim\left(A\right).$$

We have

$$\mathrm{H}\left(A \mid B\right) = \mathrm{codim}_A\left(A \cap B\right).$$

In a similar way, conditional mutual information is expressed.

We give the following definition in order to fix ideas about inequalities.

Definition 1.1.2. Let P be a proper subset of primes, and let I_1, ..., I_k be subsets of $[n]$. Let $\alpha_i \in \mathbb{R}$, for $1 \leq i \leq k$. Consider a linear inequality of the form

$$\sum_{i=1}^{k} \alpha_i \mathrm{H}\left(X_j : j \in I_i\right) \geq 0.$$

- The inequality is called a *characteristic-dependent linear rank inequality*, if it holds for

$$\begin{array}{c} A_1\ A_2\ A_3\ B_1\ B_2\ B_3\ C \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

Figure 1.1.1: A matrix over GF (p)

all jointly distributed linear random variables $X_1, \ldots, X_n$ finite fields with characteristic in P, and does not in general hold over other characteristics.

- The inequality is called a *linear rank inequality*, if it holds for all jointly distributed linear random variables over all finite field.
- The inequality is called an *information inequality*, if it holds for all jointly distributed random variables.

By definition of linear random variables, we note any information inequality is an inequality which is also satisfied by dimensions of spans of vector spaces. It is known that any unconstrained information inequality in three or fewer random variables can be written as a linear combination of instances of Shannon's inequality: $I(X;Y \mid Z) \geq 0$.

Example 1.1.3. [49] Some important inequalities:

- $\mathrm{H}(X) \leq |X|$; with equality if and only if X is an uniform distribution.
- $\mathrm{H}(X) \leq \mathrm{H}(Y)$, if $X \subseteq Y$.
- $\mathrm{H}(X \cup Y) + \mathrm{H}(X \cap Y) \leq \mathrm{H}(X) + \mathrm{H}(Y)$.

The following inequality is the first linear rank inequality which is not information inequality.

Example 1.1.4. (Ingleton's inequality [22]) For any A_1, A_2, A_3, A_4 subspaces of a finite dimensional vector space,

$$\mathrm{I}(A_1; A_2) \leq \mathrm{I}(A_1; A_2 \mid A_3) + \mathrm{I}(A_1; A_2 \mid A_4) + \mathrm{I}(A_3; A_4).$$

Remark 1.1.5. We can think a characteristic-dependent linear rank inequality like a linear rank inequality that is true over some fields.

The following example shows two characteristic-dependent linear rank inequalities obtained by the Dougherty's inverse function method.

Example 1.1.6. [14] Let $A_1, A_2, A_3, B_1, B_2, B_3$ and C be vector subspaces of a finite dimensional vector space V over a finite field $\mathbb{F}$. The following inequalities are characteristic-dependent linear rank inequalities:

- If $\mathrm{char}(\mathbb{F}) \neq 2$, then

$$\begin{aligned} &2\mathrm{H}(A_1) + \mathrm{H}(A_2) + 2\mathrm{H}(A_3) \leq \mathrm{H}(B_1) + \mathrm{H}(B_2) + \mathrm{H}(B_3) + \mathrm{H}(C) \\ &+2\mathrm{H}(A_1 \mid B_1, C) + \mathrm{H}(A_2 \mid B_2, C) + 2\mathrm{H}(A_3 \mid A_1, B_2) \\ &+3\mathrm{H}(B_2 \mid B_1, B_3) + 3\mathrm{H}(C \mid A_3, B_3) + 5\mathrm{H}(B_3 \mid A_1, A_2) + 5\mathrm{H}(B_1 \mid A_2, A_3) \\ &+5\left(\mathrm{H}(A_1) + \mathrm{H}(A_2) + \mathrm{H}(A_3) - \mathrm{H}(A_1, A_2, A_3)\right). \end{aligned}$$

- If $\mathrm{char}(\mathbb{F}) = 2$, then

$$\begin{aligned} &2\mathrm{H}(A_1) + 3\mathrm{H}(A_2) + 2\mathrm{H}(A_3) \leq \mathrm{H}(B_1) + \mathrm{H}(B_2) + \mathrm{H}(B_3) + 3\mathrm{H}(C) \\ &+2\mathrm{H}(A_1 \mid B_1, C) + 3\mathrm{H}(A_2 \mid B_2, C) + 2\mathrm{H}(A_3 \mid B_3, C) \\ &+2\mathrm{H}(B_3 \mid A_1, A_2) + 4\mathrm{H}(B_2 \mid A_1, A_3) + 3\mathrm{H}(B_1 \mid A_2, A_3) + 6\mathrm{H}(C \mid A_1, A_2, A_3) \\ &+\mathrm{H}(A_3 \mid B_1, B_2, B_3) + 7\left(\mathrm{H}(A_1) + \mathrm{H}(A_2) + \mathrm{H}(A_3) - \mathrm{H}(A_1, A_2, A_3)\right). \end{aligned}$$

These inequalities do not in general hold over other fields whose characteristic is different to the described characteristic. A counterexample would be in $V = \mathrm{GF}(p)^3$, take the generated subspaces by the columns of the matrix in Figure 1.1.1. If $p = 2$, the first inequality does not hold; and if $p \neq 2$, the second inequality does not hold. It is remarkable that these inequalities are true over any field when $\dim(V) \leq 2$.

The following example shows other two characteristic-dependent linear rank inequalities obtained from Fano and non-Fano matroids.

Example 1.1.7. [5] Let $A_1, A_2, A_3, B_1, B_2, B_3$ and C be vector subspaces of a finite dimensional vector space V over a finite field $\mathbb{F}$. The following inequalities are characteristic-dependent linear rank inequalities:

- If $\mathrm{char}(\mathbb{F}) = 2$, then

$$\begin{aligned} &\mathrm{H}(A_1, C) + \mathrm{H}(A_2, C) + \mathrm{H}(A_3, C) + 4\mathrm{H}(A_1, A_2, A_3) \\ &+3\mathrm{H}(A_1, A_2, C) + 3\mathrm{H}(A_1, A_3, C) + 3\mathrm{H}(A_2, A_3, C) + \mathrm{H}(B_1, B_2, B_3) \leq \end{aligned}$$

$$2\mathrm{H}(A_1)+2\mathrm{H}(A_2)+3\mathrm{H}(A_3)+11\mathrm{H}(C)+3\mathrm{H}(A_1,A_2)+2\mathrm{H}(A_1,A_3)+2\mathrm{H}(A_2,A_3)$$
$$+\mathrm{H}(A_1,A_2,B_3)+\mathrm{H}(A_1,A_3,B_2)+\mathrm{H}(A_2,A_3,B_1)$$
$$+\mathrm{H}(A_1,B_1,C)+\mathrm{H}(A_2,B_2,C)+\mathrm{H}(A_3,B_3,C).$$

- If $\mathrm{char}(\mathbb{F})\neq 2$, then

$$3\mathrm{H}(A_1,A_2,C)+3\mathrm{H}(A_1,A_3,C)+3\mathrm{H}(A_2A_3,C)+12\mathrm{H}(A_1,A_2,A_3)+3\mathrm{H}(A_1,B_1)$$
$$+3\mathrm{H}(A_2,B_2)+3\mathrm{H}(A_3B_3)\leq 3\mathrm{H}(A_1)+3\mathrm{H}(A_2)+9\mathrm{H}(A_3)+6\mathrm{H}(C)+6\mathrm{H}(A_1,A_2)$$
$$+3\mathrm{H}(A_1,A_2,B_3)+3\mathrm{H}(A_1,A_3,B_2)+3\mathrm{H}(A_1,B_1,C)+3\mathrm{H}(A_2,B_2,C)+3\mathrm{H}(A_3B_3,C)$$
$$+3\mathrm{H}(A_2,A_3,B_1)+3\mathrm{H}(A_1,A_2,A_3,C)+\mathrm{H}(B_1,B_2,B_3).$$

We remark that the second inequality in previous example is slightly different to the presented in [5]; we correct a mistake in that paper.

The following statement was independently proven in [10] and [18]; both demonstrations used the inverse function method.

Theorem 1.1.8. *For each finite or co-finite set of primes P, there exists a characteristic-dependent linear rank inequalities which is true over fields with characteristic in P.*

1.1.1 Partitions

To finish this section, we briefly describe a class of random variables determined by a partitions. Fixed $t\in\mathbb{N}$, a partition of a set $\mathcal{A}^t$ is denoted by $\bar{f}:=\left\{P_i\left(\bar{f}\right):\text{some } i\text{'s}\right\}$, where $P_i\left(\bar{f}\right)$ denote the i-part. The common refinement of two partitions $\bar{f}$ and $\bar{g}$ is given by the partition $\bar{f}\wedge\bar{g}$ with parts $\left\{P_i\left(\bar{f}\right)\cap P_j\left(\bar{g}\right):P_i\left(\bar{f}\right)\cap P_j\left(\bar{g}\right)\neq\phi\right\}$.

The collection of partitions of the set $\mathcal{A}^t$ and the operation $\wedge$ form a bounded semilattice, where $E_{\mathcal{A}^t}$, the partition with $|\mathcal{A}|^t$-parts, is the minimum; y $\{\mathcal{A}^t\}$, the partition with a part, is the maximum. The partial order $\bar{f}\leq\bar{g}$ is induced by $\bar{f}\wedge\bar{g}=\bar{f}$. For any $X\subseteq V=\{1,\ldots,m\}$, the common refinement of all partition $\bar{f}_v$, with $v\in X$, is

$$\bar{f}_X:=\bigwedge_{v\in X}\bar{f}_v.$$

We remark $\bar{f}_\emptyset:=\{\mathcal{A}^t\}$; $\bar{f}_{X\cup Y}=\bar{f}_X\wedge\bar{f}_Y$; $\bar{f}_{X\cup Y}\leq\bar{f}_{X\cap Y}$; $\bar{f}_Y\leq\bar{f}_X$, if $X\subseteq Y$.

The *entropy* of a partition $\bar{f}$ is the entropy of the random variable $X_{\bar{f}}$ over $\bar{f}$ given by the

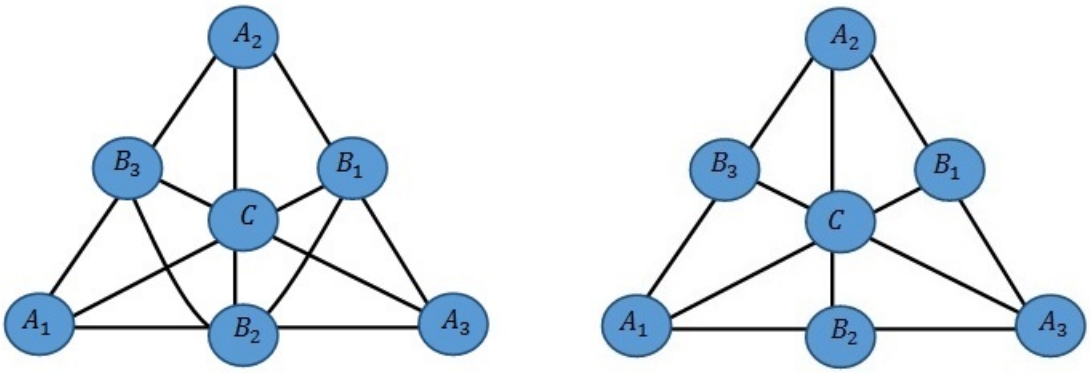

Figure 1.2.1: Fano and non-Fano Matroids

probability density function

$$\mathrm{p}\left(X_{\bar{f}} = i\text{-part}\right) = \frac{\left|P_i\left(\bar{f}\right)\right|}{|\mathcal{A}|^t}.$$

The joint random variable $\left(X_{\bar{f}}, X_{\bar{g}}\right)$ is given by $X_{\bar{f}\wedge\bar{g}}$.

When $\left|\bar{f}\right| \leq |\mathcal{A}|^n$, $\bar{f}$ can be seen as the partition of $\mathcal{A}^t$ into pre-images under some function $f : \mathcal{A}^t \to \mathcal{A}^n$. This partition is refereed as *kernel* of f, and it is used the notation $\ker(f) := \bar{f}$. We will usually work with a family $\bar{\mathcal{F}} := \left(\bar{f}_v\right)_{v\in V}$ of $|V| = m$ partitions of $\mathcal{A}^t$ with at most $|\mathcal{A}|^n$-parts. Therefore, the entropy of $\bar{f}_X$ is denoted by

$$\mathrm{H}(X) := \mathrm{H}\left(\bar{f}_X\right),$$

for $X \subseteq V$, when we fix the family $\bar{\mathcal{F}}$.

Remark 1.1.9. When $\bar{f}$ is the kernel of a linear function, this coincides with the quotient partition of f under null space. Therefore, characteristic-dependent linear rank inequalities, which are true over a field $\mathbb{F}$, hold over a family $\bar{\mathcal{F}}$ of kernel of linear functions over $\mathbb{F}$.

1.2 Matroids

A matroid is an abstract structure that captures the notion of independence that comes from Linear Algebra.

Definition 1.2.1. A *matroid* $\mathcal{M}$ is a pair $(V, \mathcal{I})$, where V is a finite set and $\mathcal{I}$ is a set of subsets of V that satisfy the following properties:

(i) $\emptyset \in \mathcal{I}$.

(ii) if $I \in \mathcal{I}$, $J \subseteq I$, then $J \in \mathcal{I}$.
(iii) if $I, J \in \mathcal{I}$ and $|J| + 1 = |I|$, then there exists $x \in I - J$, such that $J \cup x \in \mathcal{I}$.

The sets in $\mathcal{I}$ are called *independent sets*. A subset of V that is not an independent set is called *dependent*. A *circuit* is a minimal dependent subset. A *basis* is an maximal independent set and the matroid rank is the side of any base.

The rank function of a matroid is the application $r_{\mathcal{M}} : 2^V \to \mathbb{N}$, with

$$r_{\mathcal{M}}(X) = |\mathcal{B}_X|,$$

where $\mathcal{B}_X$ (or $\mathcal{B}_X^{\mathcal{M}}$) is the largest independent set contained in X. A matroid is determined by its rank function, we usually write $\mathcal{M} = (V, r_{\mathcal{M}})$ or $\mathcal{M} = (V, r)$.

A matroid can be characterized in terms of bases, circuits, closure operators (we formally define it in chapter 7) and other objects [34].

Definition 1.2.2. A matroid $\mathcal{M}$ is *representable* or *l-representable*, if there exists a matrix A with entries from some field $\mathbb{F}$ such that there is a one-to-one correspondence between the columns of A and the ground set of $\mathcal{M}$, and it holds that a set is independent in $\mathcal{M}$ if and only if the corresponding set of columns of A is linearly independent (as vectors).

Proposition 1.2.3. *[34] If a matroid is l-representable over a field, then it is l-representable over some finite field $\mathbb{F}$ and also over every extension $\mathbb{E}$ of $\mathbb{F}$.*

Example 1.2.4. We have a graphic representation in circuit terms of the Fano matroid in Figure 1.2.1 and a matrix representation over fields of even characteristic in Figure 1.1.1.

Definition 1.2.5. A matroid $\mathcal{M}$ is *partition representable* (or briefly *p-representable*) if and only if some of its positive multiples are entropic. In other words, there exist random variables Y_i, $i \in V$, and $\alpha > 0$ such that $r_{\mathcal{M}}(X) = \alpha \mathrm{H}(Y_X)$ for all $X \subseteq V$.

Equivalent definitions of p-representation are found in [46, 28, 29]. The notion of *secret sharing matroid* (*ss-representable matroid*) is equivalent to partition representation [43].

A concept associated to p-representation is the following:

Definition 1.2.6. A matroid is *ml-representable*, if for some $n \in \mathbb{N}$ there exist subspaces A_i, $i \in V$, of a vector space V over a field such that $\mathrm{H}(A_i : i \in X) = n r_{\mathcal{M}}(X)$.

If the subspaces have dimension at most 1, we have a l-representation. Obviously, ml-representable matroids are p-representable. We have [28, 34]:

$$\text{l-rep.} \subsetneq \text{ml-rep.} \subseteq \text{p-rep.} = \text{ss-rep.} \subsetneq \text{matroid} \subsetneq \text{closure operator.}$$

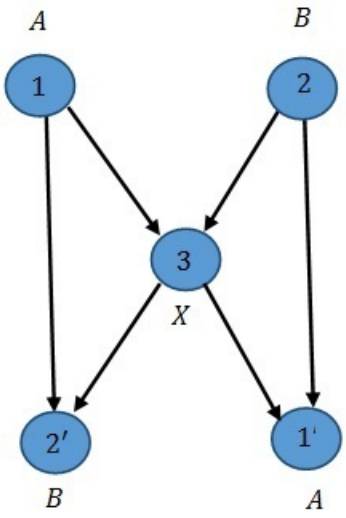

Figure 1.3.1: network coding problem of the Butterfly network.

It is an open problem to determine, if the class of ml-representable matroids is the same that the class of p-representable matroids [46]. An counterexample suggests the existence of a p-representable matroid that violates Ingleton inequality.

1.3 Network Coding

Definition 1.3.1. A *digraph* is a pair $D := (V, E)$, where $E \subseteq V^2$. The elements of V are called *nodes*; the ordered pair of E are called *edges*, and they are denoted by $e = uv$, where u and v are nodes.

Associated to a digraph, we have the following sets:

$$v^- := \{u \in V : uv \in E\},$$

$$v^+ := \{u \in V : vu \in E\},$$

and for each $X \subseteq V$,

$$X^- := \bigcup_{v \in X} v^-,$$

$$X^+ := \bigcup_{v \in X} v^+.$$

Remark 1.3.2. For nodes u, v, s, t of a graph D, we have

- v is said to be intermediate, if $v^-, v^+ \neq \emptyset$;

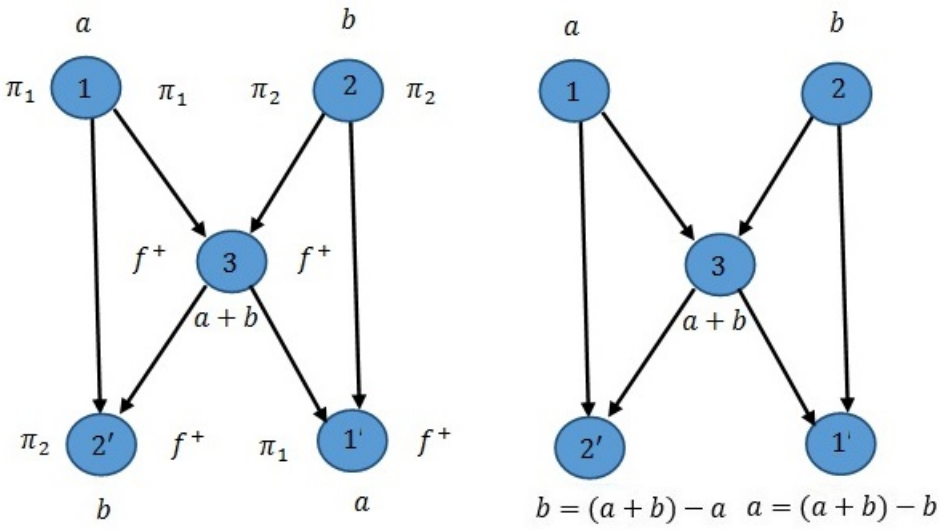

Figure 1.3.2: Butterfly network, left to right: a solution and its accumulation code; network flow.

- s is said to be source, if $s^- = \emptyset$;
- t is said to be terminal, if $t^+ = \emptyset$.
- A path of u to v is a node sequence $v_1, ..., v_k$ such that $v_i v_{i+1} \in E$, where $i = 1, ..., k-1$, $v_1 = u$ y $v_k = v$.
- A cycle is a path such that $v_1 = v_k$.

Definition 1.3.3. A digraph D is called an acyclic digraph, if it has no cycles. In this case, there always exist source and terminal nodes; the set of sources is denoted by S, and the set of terminals is denoted by T.

We now define the network coding model that we will use.

Definition 1.3.4. A *network is a pair* $\mathcal{N} = (D, \tau)$, where $D = (V, E)$ is an acyclic digraph and $\tau : T \to S$ is a surjective function called demand function.

Fractional solutions on a network have been studied in [11, 14] among other papers. We now give a formalization of this concept.

Definition 1.3.5. A (k, n)*-fractional code on* $\mathcal{N}$ *defined over an alphabet* $\mathcal{A}$ (or briefly, a (k, n)-code over $\mathcal{A}$) is a collection of functions $\mathcal{F} = (f_v)_{v \in V}$ of the form

- $f_s = \pi_s : \mathcal{A}^{|S|k} \to \mathcal{A}^k$ the canonical projection on the components indexed by s, if $v = s \in S$;

- $f_v : \mathrm{Im}(f_{v^-}) \subseteq \mathcal{A}^{|v^-|} \to \mathcal{A}^n$, where $\mathrm{Im}(f_{v^-}) := \mathrm{Im}(f_{v_1}) \times \cdots \times \mathrm{Im}(f_{v_l})$, $v^- = \{v_1, ..., v_l\}$, if $v \in V - (S \cup T)$;
- $f_t : \mathrm{Im}(f_{t^-}) \to \mathcal{A}^k$, if $v = t \in T$.

A *message* is an element of $\mathcal{A}^k$. We consider a tuple of messages $x \in \mathcal{A}^{|S|k}$. Each tuple of messages can be written as

$$x = \left(x_{s_1}, ..., x_{s_{|S|}}\right) := \left(x_1, ..., x_{|S|}\right),\ S = \left\{s_1, ..., s_{|S|}\right\},$$

where $x_i = \pi_s(x)$ is the message of s_i. The functions f_t, $t \in T$, are called *decoding functions*. A (k, n)-code is *linear*, if $\mathcal{A}$ is a finite field and each f_v is a linear function.

Remark 1.3.6. The source s has the message x_s and has no information about the messages $x_{s'}$, with $s' \neq s$.

The following concept is given as an auxiliary definition to express when a code is a solution.

Definition 1.3.7. The *accumulation code* of a (k, n)-code $\mathcal{F}$ is a collection of functions $\mathcal{F}^* = (f_v^*)_{v \in V}$ of the form

- $f_s^* := f_s$, if $v = s \in S$;
- $f_v^*(x) := f_v(f_{v^-}^*(x)) := f_v\left((f_w^*(x))_{w \in v^-}\right)$ for each $x \in \mathcal{A}^{|S|k}$, if $v \in V - S$.

Remark 1.3.8. Each f_v^* is defined in an inductive way from each node of v^-. Also, the vector $f_v^*(x)$ is the message of v in the code $\mathcal{F}$ for the tuple of messages x.

Definition 1.3.9. A (k, n)-code over $\mathcal{A}$ is said to be a (k, n)-fractional solution on $\mathcal{N}$ defined over $\mathcal{A}$ (or briefly, a (k, n)-solution over $\mathcal{A}$), if for every tuple of messages $x \in \mathcal{A}^{|S|k}$,

$$f_t^*(x) = x_{\tau(t)}\ \forall t \in T.$$

The parameter more important in a network is the capacity:

Definition 1.3.10. The *capacity of* $\mathcal{N}$ *respect to a class of codes* $\mathcal{D}$ *over* $\mathcal{A}$ is

$$\mathrm{C}_{\mathcal{D}}^{\mathcal{A}}(\mathcal{N}) := \sup\left\{\frac{k}{n} :\ \exists \text{ a } (k, n)\text{-solution in } \mathcal{D}\right\}.$$

The class of codes $\mathcal{D}$ is usually though as the collection of all codes (denoted by $\mathrm{C}(\mathcal{N})$), in this case the capacity is usually refereed as *non-linear coding capacity*. Also $\mathcal{D}$ can be taken as the collection of linear codes over determined finite fields (or over any finite field).

The network coding problem of $\mathcal{N}$ consists in finding some alphabet and an efficient solution over this alphabet; the efficiency is measured by the rate $\frac{k}{n}$. Therefore we are interesting in the value of $\mathrm{C}_{\mathcal{D}}^{\mathcal{A}}(\mathcal{N})$ and solutions that can achieve this.

Remark 1.3.11. [11, 12] A network is defined to be:

- *Solvable over* $\mathcal{A}$, if there exists a $(1,1)$-solution over $\mathcal{A}$; and *solvable*, if the network is solvable over some $\mathcal{A}$. In this case, $\mathrm{C}(\mathcal{N}) = \mathrm{C}^{\mathcal{A}}(\mathcal{N}) = 1$ and the capacity is achievable.

- *Scalar linearly solvable over* $\mathbb{F}$, if there exists a $(1,1)$-linear solution over $\mathbb{F}$; and *scalar linearly solvable*, if the network is scalar linearly solvable over some $\mathbb{F}$. In this case, $\mathrm{C}(\mathcal{N}) = \mathrm{C}_{\text{scalar linear}}^{\mathbb{F}}(\mathcal{N}) = 1$ and the capacity is achievable.

- *(Vector) Linearly solvable over* $\mathbb{F}$, if there exists a (k,k)-linear solution over $\mathbb{F}$, for some $k \geq 1$; *and linearly solvable*, if the network is (vector) linearly solvable over some $\mathbb{F}$. In this case, $\mathrm{C}(\mathcal{N}) = \mathrm{C}_{\text{linear}}^{\mathbb{F}}(\mathcal{N}) = \mathrm{C}_{\text{scalar linear}}^{\mathbb{F}}(\mathcal{N}) = 1$ and the capacity is achievable.

- *Asymptotically solvable over* $\mathcal{A}$, if for any $\epsilon > 0$, there exists a (k,n)-solution over $\mathcal{A}$ such that $\frac{k}{n} > 1 - \epsilon$; and the network is *asymptotically solvable*, if the network is asymptotically solvable over some $\mathcal{A}$. In this case, $\mathrm{C}(\mathcal{N}) = \mathrm{C}^{\mathcal{A}}(\mathcal{N}) = 1$ but we do not know if there exists a solution with rate 1.

- *Asymptotically linearly solvable over* $\mathbb{F}$, if for any $\epsilon > 0$, there exists a (k,n)-linear solution over $\mathbb{F}$ such that $\frac{k}{n} > 1 - \epsilon$; and the network is *asymptotically linearly solvable*, if the network is asymptotically linearly solvable over some $\mathbb{F}$. In this case, $\mathrm{C}(\mathcal{N}) = \mathrm{C}^{\mathbb{F}}(\mathcal{N}) = 1$ but we do not know if there exists a linear solution with rate 1.

A *multiple-unicast network* is a network $\mathcal{N}$ whose demand function is bijective. In such a case, $\tau(t_i) = s_i$, for $i = 1, \ldots, r := |S|$, and we simply write $\mathcal{N} := (D, S, T)$. A (k,n)-code is a solution, if for every $x = (x_1, ..., x_r) \in \mathcal{A}^r$, $f_{t_i}^*(x) = x_i$ for each i. In other words, $f_T^* = \mathrm{id}_{\mathcal{A}^{rk}}$. It is known that the problem of determining whether a network is solvable can be reduced to the study of a multiple-unicast network as shows the following theorem.

Theorem 1.3.12. [15] *For every network* $\mathcal{N}$*, there exists a multiple-unicast network* $\mathcal{N}'$ *such that*

- $\mathcal{N}$ *is solvable over* $\mathcal{A}$ *if and only if* $\mathcal{N}'$ *is solvable over* $\mathcal{A}$*.*

- $\mathcal{N}$ *is linearly solvable over* $\mathbb{F}$ *if and only if* $\mathcal{N}'$ *is linearly solvable over* $\mathbb{F}$*.*

We next write the solvability network coding problem in terms of partitions for multiple-unicast network.

Theorem 1.3.13. *Let $\mathcal{N}$ be a multiple-unicast network. We have that $\mathcal{N}$ has a (k,n)-solution over $\mathcal{A}$ if and only if there exists a family of partitions $\bar{\mathcal{F}} = \left(\bar{f}_v\right)_{v\in V}$ on $\mathcal{A}^{rk}$ such that*

(i) $\left|\bar{f}_v\right| = |\mathcal{A}|^k$, *for* $v = s \in S$.

(ii) $\left|\bar{f}_v\right| \leq |\mathcal{A}|^n$, *for* $v \in V - (S \cup T)$.

(iii) $\bar{f}_{s_i} = \bar{f}_{t_i}$, *for each* i.

(iv) $\bar{f}_{v^-} \leq \bar{f}_v$, *for* $v \in V - S$.

(v) $\left|\bar{f}_T\right| = |\mathcal{A}|^{rk}$.

Proof. Let $\mathcal{F} = (f_v)_{v\in V}$ be a (k,n)-solution over $\mathcal{A}$, and define $\bar{f}_v := \ker(f_v^*)$. We have to show that $\bar{\mathcal{F}} = \left(\bar{f}_v\right)_{v\in V}$ is the desired family of partitions. (i) and (ii) are immediate from the definition of code; (iii) and (v) are also true because the code is a solution. It remains to prove item (iv), let $x_{v^-} \in f_{v^-}^*\left(\mathcal{A}^{rk}\right)$ and take $y \in f_{v^-}^{*-1}(x_{v^-})$. So, $f_{v^-}^*(y) = x_{v^-}$. Since $\bar{\mathcal{F}}$ is a code we have $f_v^*(y) = f_v\left(f_{v^-}^*(y)\right) = f_v(x_{v^-})$. So, we can define $x_v := f_v(x_{v^-})$ to obtain that $y \in f_v^{*-1}(x_v)$. In other words, $f_{v^-}^{*-1}(x_{v^-}) \subseteq f_v^{*-1}(x_v)$. Therefore, $\bar{f}_{v^-} \leq \bar{f}_v$. Reciprocally, let $\bar{\mathcal{F}} = \left(\bar{f}_v\right)_{v\in V}$ be a family of partitions that holds the described conditions. (i), (iii) and (v) imply that $\bar{f}_v = \ker(\pi_v)$ for each $v \in S \cup T$; in these cases, we define $f_v^* := \pi_v$. (i) implies that each $\bar{f}_v$, $v \in V - (S \cup T)$, is the kernel of a function f_v^* from $\mathcal{A}^{rk}$ to $\mathcal{A}^n$. The proof is completed showing that $\mathcal{F}^* = (f_v^*)_{v\in V}$ is the accumulation code of a (k,n)-solution over $\mathcal{A}$. From (iv), for any $v \in V - S$ and $x_{v^-} \in f_{v^-}^*\left(\mathcal{A}^{rk}\right)$, there exists unique $x_v \in f_v^*\left(\mathcal{A}^{rk}\right)$ such that $f_{v^-}^{*-1}(x_{v^-}) \subseteq f_v^{*-1}(x_v)$. Define the function f_v by $f_v(x_{v^-}) := x_v$. Note that $f_v^*(x) = f_v\left(f_{v^-}^*(x)\right)$ and $f_{t_i}^*(x) = \pi_{s_i}(x) = x_{s_i}$, for all $x \in \mathcal{A}^{rk}$ and i. Therefore, $\mathcal{F}$ is a solution. □

Example 1.3.14. [36] In Figure 1.3.1 is shown the Butterfly network. In Figure 1.3.2 (left), there is a solution and its accumulation code over $\mathcal{A} = \mathrm{GF}(2)$, where f^+ is the sum function, π_i is the i-projection on $\mathrm{GF}(2)^2$; the functions of the solution are shown to the right of each node, and its accumulation code is shown to the left of each node. In the same figure (right), it is shown its flow information. One can check that the associated partitions to this solution hold the conditions of previous theorem as presented in Figure 1.3.3.

1.4 Secret Sharing

Secret Sharing is an area of Information Theory and a useful tool that appears as a important component in many kinds of cryptographic protocols [44, 6, 35, 17]. In a *secret sharing*

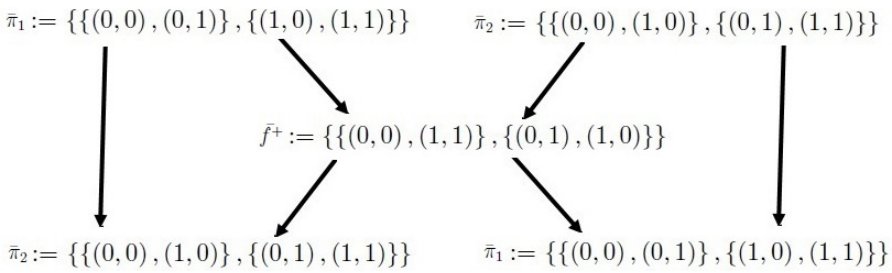

Figure 1.3.3: A solution of the Butterfly network in terms of partitions

scheme, a *secret value* is distributed into *shares* among a set of *participants* in such a way that only the *qualified sets* of participants can recover the secret value.

Definition 1.4.1. An *access structure*, denoted by Γ on a set of participants P, is a monotone increasing family of subsets of P. Consider a special participant $p \notin P$, called dealer. A *secret sharing scheme* on P with access structure Γ is a random vector $\Sigma := (S_x)_{x \in Q}$, where $Q = P \cup p$, such that the following properties are satisfied:

(i) $\mathrm{H}(S_p) > 0$.

(ii) If $A \in \Gamma$, then $\mathrm{H}(S_p \mid S_A) = 0$.

(iii) If $A \notin \Gamma$, then $\mathrm{I}(S_p; S_A) = 0$.

The random variable S_p is the *secret value*, and the *shares* received by the participants are given by the random variables S_x, $x \in P$. A set of participants A is said to be *qualified* or *authorized*, if $A \in \Gamma$; and it is said to be *non-qualified* or *non-authorized*, if $A \notin \Gamma$. A *minimal qualified set* is a qualified set such that any proper subset is non-qualified. It is clear that an access structure is determined by the family $\min \Gamma$ of its minimal qualified sets.

Definition 1.4.2. The *information ratio* $\sigma(\Sigma)$ of the secret sharing scheme Σ is given by

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

The *optimal information ratio* $\sigma(\Gamma)$ of an access structure Γ is the infimum of the information ratios of all secret sharing schemes for Γ; the optimal information ratio, when the random variables are linear, is denoted by $\lambda(\Gamma)$.

Definition 1.4.3. A secret sharing scheme $\Sigma = (S_x)_{x \in Q}$ is said to be *ideal*, if its information ratio is equal to 1. An access structure that admits an ideal secret sharing scheme is called *ideal access structure*.

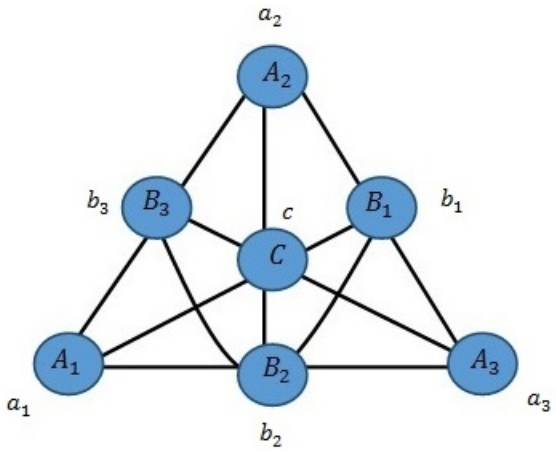

Figure 1.4.1: Fano matroid defines a access structure on six participants

Matroids are related to secret sharing:

Definition 1.4.4. Let $\mathcal{M} = (V, r)$ be a matroid. The *port* of the matroid $\mathcal{M}$ at $p \in Q := V$ is the access structure on $P = Q - p$ whose qualified sets are the sets $X \subseteq P$ satisfying $r(X \cup p) = r(X)$.

The following result connects ideal secret sharing and matroids.

Theorem 1.4.5. *Let $\Sigma = (S_x)_{x \in Q}$ be an ideal secret sharing scheme on P with access structure Γ. Then, the mapping given by $f(X) = \frac{\mathrm{H}(S_X)}{\mathrm{H}(S_p)}$ for each $X \subseteq Q$ is the rank function of a matroid $\mathcal{M}$ with ground set Q. Moreover, Γ is the port of the matroid $\mathcal{M}$ at p.*

As a consequence, every ideal access structure is a matroid port. In fact, the matroids in Theorem 1.4.5 are p-representable. It is known that Vámos matroid is not p-representable. Therefore the ports of the Vámos matroid are counterexamples for the converse [43].

Example 1.4.6. [28, 23] The port of the Fano matroid at c, according Figure 1.4.1, is given by the minimum authorized sets:

$$\min \mathcal{F} := \{a_1b_1, a_2b_2, a_3b_3, a_1a_2a_3, a_1b_2b_3, b_1a_2b_3, b_1b_2a_3\}.$$

We can check that the columns of a matrix of representation of Fano matroid define a ideal linear secret sharing scheme over fields whose characteristic is two, and therefore the ports of the Fano matroid are ideal. We have $\sigma(\mathcal{F}) = 1$. It is more hard to show that $\lambda(\mathcal{F}) = \frac{4}{3}$ for fields whose characteristic is other than two.

2 Method I for Producing Inequalities

In this chapter, we show a method to produce characteristic-dependent linear rank inequalities using as guide binary matrices whose rank is different according to the choice of the characteristic of the field where its inputs are defined. We first introduce some important concept about complementary vector spaces. Next, we present a particular case of the method: we exhibit a 10×10 binary matrix whose rank is 8 over fields with characteristic 2; 9 over fields with characteristic 3; and 10 over fields with characteristic neither 2 nor 3. Then, we produce three inequalities: the first is true over fields with characteristic 2; the second is true over fields with characteristic 2 or 3; and the third is true over fields with characteristic neither 2 nor 3. By last, we summarize the method through a theorem with a proof that is valid for any binary matrix whose rank is as we have described; we show some consequences and produce additional inequalities using some specific families of matrices. We remark that this method is deeply based on the technique used by Blasiak et al. for producing two characteristic-dependent linear rank inequalities using as a guide the Fano and non-Fano matroids [5].

2.1 How to use a binary matrix

Definition 2.1.1. Let A and B be vector subspaces of a finite dimensional vector space V. We say that $A + B$ is a *direct sum*, denoted by $A \oplus B$, if $A \cap B = O := \langle O \rangle$.

In case that $V = A \oplus B$, the members of this sum are called *(mutually) complementary subspaces* in V. Alternatively, A_1, ..., A_n are mutually complementary subspaces in V, if every vector of V has an unique representation as a sum of elements of A_1, ..., A_n. In this case, π_I denotes the *I-projection function* $V \twoheadrightarrow \bigoplus_{i \in I} A_i$ given by

$$x = \sum_{i=1}^{n} x_i \mapsto \sum_{i \in I} x_i.$$

Definition 2.1.2. Let $V = A_1 \oplus \cdots \oplus A_n$, and take a vector subspace C of V such that $A_1 + \cdots + A_{i-1} + C + A_{i+1} + \cdots + A_n$ is a direct sum for all i. We say that $(A_1, \ldots, A_n, C)$

is *a tuple of complementary vector subspaces in* V.

Example 2.1.3. In $V = \mathrm{GF}(p)^6$, take $A_1 = \langle e_1, e_4\rangle$, $A_2 = \langle e_2, e_5\rangle$, $A_3 = \langle e_3, e_6\rangle$ and $C = \langle e_1 + e_2 + e_3, e_4 + e_4 + e_6\rangle$. Then, (A_1, A_2, A_3, C) is a tuple of complementary vector subspaces in V.

Proposition 2.1.4. *For any tuple* $(A_1, \ldots, A_n, C)$ *of complementary vector subspaces in* V*, we have*

$$\mathrm{H}(\pi_I(C)) = \mathrm{H}(C) \leq \mathrm{H}(A_i),$$

for all i *and* $\emptyset \neq I \subseteq [n]$.

Proof. Let $x \in C$ such that $\pi_I(x) = O$. So, $\sum\limits_{i\in I} x_i = O$. Hence, $x \in \bigoplus\limits_{i\notin I} A_i$. By definition of tuple of complementary vector spaces, $x = O$. In other words, $\pi_I(C)$ and C are isomorphic or have the same dimension. It remains the last inequality. We note

$$\begin{aligned}\mathrm{H}(C) + \mathrm{H}(A_1, \ldots, A_{i-1}, A_{i+1} \ldots, A_n) &= \mathrm{H}(A_1, \ldots, A_{i-1}, C, A_{i+1} \ldots, A_n)\\ &\leq \mathrm{H}(A_1, A_2, \ldots, A_n)\\ &\leq \mathrm{H}(A_i) + \mathrm{H}(A_1, \ldots, A_{i-1}, A_{i+1} \ldots, A_n).\end{aligned}$$

So $\mathrm{H}(C) \leq \mathrm{H}(A_1)$. □

Corollary 2.1.5. *A non-zero* $c \in C$ *can be uniquely written in form* $a_1 + \cdots + a_n$ *where each* a_i *is non-zero.*

Proposition 2.1.6. *For any* A_1, …, A_n *and* C *vector subspaces of a finite dimensional vector space* V*, there exists a tuple of complementary vector subspaces* $\left(\bar{A}_1, \ldots, \bar{A}_n, \bar{C}\right)$ *such that* $\bar{A}_i \leq A_i$, $\bar{C} \leq C$, $\bigoplus \bar{A}_i = \sum A_i$ *and*

$$\mathrm{H}\left(A_i \mid \bar{A}_i\right) = \mathrm{I}\left(A_{[i-1]}; A_i\right)$$

$$\mathrm{H}\left(C \mid \bar{C}\right) \leq \mathrm{H}\left(C \mid A_{[n]}\right) + \sum_{i=1}^{n} \mathrm{I}\left(A_{[n]-i}; C\right).$$

Proof. We first build mutually complementary subspaces $\bar{A}_1$,..., $\bar{A}_n$ in $A_{[n]}$ from $A_1, ..., A_n$. Define $\bar{A}_1 := A_1$, and for $i = 2, \ldots, n$ denote by $\bar{A}_i$ a subspace of A_i which is a complementary subspace to $A_{[i-1]}$ in $A_{[i]}$. Then $\bar{A}_1$, ..., $\bar{A}_n$ are mutually complementary and the following equations hold:

$$\mathrm{H}\left(A_i \mid \bar{A}_i\right) = \mathrm{I}\left(A_{[i-1]}; A_i\right),$$

where $A_0 = O$. Second, we built a subspace $\bar{C}$ of $C \cap \bar{A}_{[n]}$ such that $\bar{C}$ and $\bar{A}_{[n]-i}$ form a direct sum for all i. Let $C^{(0)} := C \cap A_{[n]}$. Recursively, for $i = 1, \ldots, n$ denote by $C^{(i)}$ a subspace of $C^{(i-1)}$ which is a complementary subspace to $\bar{A}_{[n]-i}$ in $C^{(i-1)} + \bar{A}_{[n]-i}$. We denote $\bar{C} := C^{(n)}$, this space satisfies the required condition and the following equation:

$$\mathrm{H}\left(C \mid C^{(0)}\right) \leq \mathrm{H}\left(C \mid A_{[10]}\right),$$

$$\mathrm{H}\left(C^{(0)} \mid \bar{C}\right) \leq \sum_{i=1}^{10} \mathrm{I}\left(A_{[n]-i}; C\right),$$

which implies,

$$\mathrm{H}\left(C \mid \bar{C}\right) \leq \mathrm{H}\left(C \mid A_{[n]}\right) + \sum_{i=1}^{n} \mathrm{I}\left(A_{[n]-i}; C\right).$$

□

Remark 2.1.7. The tuple is not unique but we will fix one of these.

The inequalities of the following lemmas, that we will use later, are valid for linear random variables that hold some additional conditions. We remark that we use the following notation of intervals:

$$[j, k] := \{i \in \mathbb{N} : j \leq i \leq k\},$$

$$[k] = [1, k].$$

The sum $A_j + \cdots + A_k$ is denoted by $A_{[j,k]}$, and $A_0 := A_\emptyset := O$.

Lemma 2.1.8. *For any subspaces $A_1, \ldots, A_n$, $A'_1, \ldots, A'_n$ of finite dimensional vector space V such that $A'_i \leq A_i$, we have*

$$\mathrm{H}\left(A_{[n]} \mid A'_{[n]}\right) \leq \sum_{i \in [n]} \mathrm{H}\left(A_i \mid A'_i\right),$$

with equality if and only if $A_{i+1} \cap A_{[i]} = A'_{i+1} \cap A'_{[i]}$ for all i.

Proof. By induction over n. In case $n = 2$, we have

$$\mathrm{H}\left(A_{[2]} \mid A'_{[2]}\right) = \mathrm{H}\left(A_{[2]}\right) - \mathrm{H}\left(A'_{[2]}\right)$$

$$= \mathrm{H}(A_1) + \mathrm{H}(A_2 \mid A_1) - \mathrm{H}(A'_1) - \mathrm{H}(A'_2 \mid A'_1)$$

$$= \mathrm{H}(A_1 \mid A'_1) + \mathrm{H}(A_2) - \mathrm{H}(A'_2) - \mathrm{I}(A_1; A_2) + \mathrm{I}(A'_1; A'_2)$$

$$= \mathrm{H}(A_1 \mid A'_1) + \mathrm{H}(A_2 \mid A'_2) + (\mathrm{I}(A'_1; A'_2) - \mathrm{I}(A_1; A_2))$$

$$\leq \mathrm{H}(A_1 \mid A_1') + \mathrm{H}(A_2 \mid A_2') \quad [\text{because } A_i' \leq A_i].$$

The equality holds if and only if $\mathrm{I}(A_1; A_2) = \mathrm{I}(A_1'; A_2')$. In other words, $A_1 \cap A_2 = A_1' \cap A_2'$ because $A_i' \leq A_i$. Now, we suppose the case $n-1$ is true. We have

$$\mathrm{H}\left(A_{[n]} \mid A'_{[n]}\right) = \mathrm{H}\left(A_{[n-1]\cup n} \mid A'_{[n-1]\cup n}\right)$$

$$\leq \mathrm{H}\left(A_{[n-1]} \mid A'_{[n-1]}\right) + \mathrm{H}(A_n \mid A_n') \quad [\text{from case } n=2]$$

$$\leq \sum_{i\in[n]} \mathrm{H}(A_i \mid A_i') \quad [\text{from case } n-1].$$

The equality holds if and only if $\mathrm{I}\left(A_{i+1}; A_{[i]}\right) = \mathrm{I}\left(A'_{i+1}; A'_{[i]}\right)$. Since $A_i' \leq A_i$ for all i, we have $A_{i+1} \cap A_{[i]} = A'_{i+1} \cap A'_{[i]}$. □

Lemma 2.1.9. *For any subspaces A, B , C of a finite dimensional vector space V such that $B \leq A$, we have*

$$\mathrm{H}(A \cap C \mid B \cap C) \leq \mathrm{H}(A \mid B),$$

with equality if and only $A + C = B + C$.

Proof. We have

$$\mathrm{H}(A \cap C \mid B \cap C) = \mathrm{H}(A \cap C) - \mathrm{H}(B \cap C)$$

$$= \mathrm{I}(A; C) - \mathrm{I}(B; C)$$

$$= \mathrm{H}(A) - \mathrm{H}(B) - \mathrm{H}(A, C) + \mathrm{H}(B, C)$$

$$\leq \mathrm{H}(A \mid B) \quad [\text{because } B \leq A].$$

The equality holds if and only if $\mathrm{H}(A, C) = \mathrm{H}(B, C)$. That is equivalent to $A + C = B + C$ since $B + C \leq A + C$. □

2.1.1 A particular case

We obtain three characteristic-dependent linear rank inequalities using as a guide the matrix in Figure 2.1.1. We only write some demonstrations because in the other section, we will present and demonstrate stronger propositions.

Let B be the 10×10 binary matrix in Figure 2.1.1. We calculate the rank of the matrix B over different fields to find:

$$\mathrm{rank}(B) = \begin{cases} 8, & \mathrm{char}(\mathbb{F}) = 2. \\ 9, & \mathrm{char}(\mathbb{F}) = 3. \\ 10, & \text{otherwise.} \end{cases}$$

$$\begin{array}{c} \begin{array}{cccccccccc} b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 & b_8 & b_9 & b_{10} \end{array} \\ \left(\begin{array}{cccccccccc} 0 & 1 & 1 & & & & & & & \\ 1 & 0 & 1 & & O_{3\times 3} & & & O_{3\times 4} & & \\ 1 & 1 & 0 & & & & & & & \\ & & & 0 & 1 & 1 & & & & \\ & O_{3\times 3} & & 1 & 0 & 1 & & O_{3\times 4} & & \\ & & & 1 & 1 & 0 & & & & \\ & & & & & & 0 & 1 & 1 & 1 \\ & O_{4\times 3} & & & O_{4\times 3} & & 1 & 0 & 1 & 1 \\ & & & & & & 1 & 1 & 0 & 1 \\ & & & & & & 1 & 1 & 1 & 0 \end{array} \right) \end{array}.$$

Figure 2.1.1: A 10×10 binary matrix.

We choose this matrix because it is the smallest binary matrix, which we find, whose rank is different over at least three different finite fields.

For a column b_i of B, the set $\left\{ j : b_i^j = 1 \right\} \subseteq [10]$ is denoted by $\bar{b}_i$; if there is no confusion, by abuse of notation, we identify b_i and $\bar{b}_i$ (for any binary matrix, we also make this). For row and column vectors, the notation is the same.

The following lemma is derived of the dependence of the rank of B to the choice of the characteristic of the finite field. We show a direct proof.

Lemma 2.1.10. *If $(A_1, \ldots, A_{10}, C)$ is a tuple of complementary vector subspaces of V, then*

$$\mathrm{H}\left(\pi_{b_i}(C) : i \in [10]\right) = \begin{cases} 8\mathrm{H}(C), & \mathrm{char}(\mathbb{F}) = 2. \\ 9\mathrm{H}(C), & \mathrm{char}(\mathbb{F}) = 3. \\ 10\mathrm{H}(C), & \textit{otherwise.} \end{cases}$$

Proof. We consider the case $\mathrm{char}(\mathbb{F}) = 2$. For any $v = \sum_{i=1}^{10} v_i \in V$, taking into account that $2 = 0$ in $\mathbb{F}$, we get $\pi_{b_3}(v) = \pi_{b_1}(v) + \pi_{b_2}(v)$ and $\pi_{b_6}(v) = \pi_{b_4}(v) + \pi_{b_5}(v)$. Hence,

$$\pi_{b_3}(C) + \pi_{b_6}(C) \leq \pi_{b_1}(C) + \pi_{b_2}(C) + \pi_{b_4}(C) + \pi_{b_5}(C) + \sum_{i=7}^{10} \pi_{b_i}(C).$$

Furthermore, the subspaces of the right side form a direct sum. In effect, let $v_i = \sum_{j=1}^{10} v_i^j \in C$, $i \in [10] - \{3, 6\}$ such that

$$\pi_{b_1}(v_1) + \pi_{b_2}(v_2) + \pi_{b_4}(v_4) + \pi_{b_5}(v_5) + \pi_{b_7}(v_7) + \pi_{b_8}(v_8) + \pi_{b_9}(v_9) + \pi_{b_{10}}(v_{10}) = O,$$

we have to show that $v_i = O$ for all i. From the equation, we get the system of equations:

$$v_2^1 = v_1^2 = v_5^4 = v_4^5 = v_1^3 + v_2^3 = v_4^6 + v_5^6 = 0,$$
$$v_8^7 + v_9^7 + v_{10}^7 = v_7^8 + v_9^8 + v_{10}^8 = v_7^9 + v_8^9 + v_{10}^9 = v_7^{10} + v_8^{10} + v_9^{10} = 0.$$

From Corollary 2.1.5, this implies the system of equations:

$$v_1 = v_2 = v_4 = v_5 = v_8 + v_9 + v_{10} = v_7 + v_9 + v_{10} = v_7 + v_8 + v_{10} = v_7 + v_8 + v_9 = 0.$$

Solving this system of equations in characteristic two, we get $v_i = O$ for all i. Now, applying proposition 2.1.5, we get

$$\mathrm{H}\left(\pi_{b_i}(C) : i \in [10]\right) = \mathrm{H}\left(\pi_{b_i}(C) : i \in [10] - \{3,6\}\right) = 8\mathrm{H}(C).$$

For the rest of the cases, we can apply a similar argument: for $\mathrm{char}(\mathbb{F}) = 3$, we can get

$$\pi_{b_{10}}(C) \leq \bigoplus_{i=1}^{9} \pi_{b_i}(C),$$

and for $\mathrm{char}(\mathbb{F}) \neq 2, 3$, we can get the sum of all those subspaces is direct. □

The following lemma is guided by the dependence relationship presented in the columns of B. We omit the proof because a more general statement will be proven in the next section.

Proposition 2.1.11. *Let A_1, ..., A_{10}, B_1, ..., B_{10} and C vector subspaces of a finite dimensional vector space V over a finite field $\mathbb{F}$ such that $(A_1, \ldots, A_{10}, C)$ is a tuple of complementary vector spaces. Consider the following conditions:*

(i) $B_i \leq \sum_{j=1, j\neq i}^{3} A_j$, $i \in [3]$; $B_i \leq \sum_{j=4, j\neq i}^{6} A_j$, $i \in [4,6]$; $B_i \leq \sum_{j=7, j\neq i}^{10} A_j$, $i \in [7,10]$.

(ii) $B_i \leq C + A_i + \sum_{j=4}^{10} A_j$, $i \in [3]$; $B_i \leq C + A_i + \sum_{j=1}^{3} A_j + \sum_{j=7}^{10} A_j$, $i \in [4,6]$;

$B_i \leq C + A_i + \sum_{j=1}^{6} A_j$, $i \in [7,10]$.

(iii) $C \leq B_i + A_i + \sum_{j=4}^{10} A_j$, $i \in [3]$; $C \leq B_i + A_i + \sum_{j=1}^{3} A_j + \sum_{j=7}^{10} A_j$, $i \in [4,6]$;

$C \leq B_i + A_i + \sum_{j=1}^{6} A_j$, $i \in [7,10]$.

We have the following implications:

1. *If conditions (i) and (ii) hold, and the characteristic of* $\mathbb{F}$ *is* 2*, then* $\mathrm{H}\left(B_{[10]}\right) \leq 8\mathrm{H}\left(C\right)$.
2. *If conditions (i) and (ii) hold, and the characteristic of* $\mathbb{F}$ *is* 3*, then* $\mathrm{H}\left(B_{[10]}\right) \leq 9\mathrm{H}\left(C\right)$.
3. *If conditions (i) and (iii) hold, and the characteristic of* $\mathbb{F}$ *is neither* 2 *nor* 3*, then* $10\mathrm{H}\left(C\right) \leq \mathrm{H}\left(B_{[10]}\right)$.

Define the following values:

$$\Delta\left(A_{[10]}\right) := \mathrm{I}\left(A_1; A_2\right) + 2\mathrm{I}\left(A_{[3]}; A_{[4,10]}\right) + \mathrm{I}\left(A_{[2]}; A_{[3,10]}\right)$$

$$+2\mathrm{I}\left(A_{[6]}; A_{[7,10]}\right) + \mathrm{I}\left(A_{[4]}; A_5\right) + \mathrm{I}\left(A_{[5]}; A_{[6,10]}\right) + \sum_{i=8}^{10} \mathrm{I}\left(A_{[i-1]}; A_i\right),$$

$$\nabla\left(A_{[10]}\right) := \sum_{(j,k)\in S} \sum_{i=j}^{k} \left[\mathrm{I}\left(A_{[j-1]}; A_{[j,i-1]}\right) + \mathrm{I}\left(A_{[i]}; A_{[i+1,k]}\right)\right],$$

where S is the set of the three points $(1,3)$, $(4,6)$, $(7,10)$. We have the following inequalities.

Theorem 2.1.12. *Let* A_1, ..., A_{10}, B_1, ..., B_{10} *and* C *be vector subspaces of a finite dimensional vector space* V *over a finite field* $\mathbb{F}$*. The following inequalities are characteristic-dependent linear rank inequalities:*

- If the characteristic of $\mathbb{F}$ *is* 2*, then*

$$\mathrm{H}\left(B_{[10]}\right) \leq 8\mathrm{I}\left(A_{[10]}; C\right) + \mathrm{H}\left(B_1 \mid A_{[2,3]}\right) + \mathrm{H}\left(B_2 \mid A_{1\cup 3}\right) + \mathrm{H}\left(B_3 \mid A_{[2]}\right)$$

$$+\mathrm{H}\left(B_4 \mid A_{[5,6]}\right) + \mathrm{H}\left(B_5 \mid A_{4\cup 6}\right) + \mathrm{H}\left(B_6 \mid A_{[4,5]}\right) + \mathrm{H}\left(B_7 \mid A_{[8,10]}\right) + \mathrm{H}\left(B_8 \mid A_{7\cup[9,10]}\right)$$

$$+\mathrm{H}\left(B_9 \mid A_{[7,8]\cup 10}\right) + \mathrm{H}\left(B_{10} \mid A_{[7,9]}\right) + \mathrm{H}\left(B_1 \mid A_{1\cup[4,10]}, C\right) + \mathrm{H}\left(B_2 \mid A_{2\cup[4,10]}, C\right)$$

$$+\mathrm{H}\left(B_3 \mid A_{3\cup[4,10]}, C\right) + \mathrm{H}\left(B_4 \mid A_{[1,3]\cup 4\cup[7,10]}, C\right) + \mathrm{H}\left(B_5 \mid A_{[1,3]\cup 5\cup[7,10]}, C\right)$$

$$+\mathrm{H}\left(B_6 \mid A_{[1,3]\cup 6\cup[7,10]}, C\right) + \mathrm{H}\left(B_7 \mid A_{[1,7]}, C\right) + \mathrm{H}\left(B_8 \mid A_{[1,6]\cup 8}, C\right) + \mathrm{H}\left(B_9 \mid A_{[1,6]\cup 9}, C\right)$$

$$+\mathrm{H}\left(B_{10} \mid A_{[1,6]\cup 10}, C\right) + 10\left[\mathrm{H}\left(C \mid A_{[10]}\right) + \sum_{i=1}^{10} \mathrm{I}\left(A_{[10]-i}; C\right)\right] + \Delta\left(A_{[10]}\right) + \nabla\left(A_{[10]}\right).$$

- If the characteristic of $\mathbb{F}$ *is* 2 *or* 3*, then*

$$\mathrm{H}\left(B_{[10]}\right) \leq 9\mathrm{I}\left(A_{[10]}; C\right) + \mathrm{H}\left(B_1 \mid A_{[2,3]}\right) + \mathrm{H}\left(B_2 \mid A_{1\cup 3}\right) + \mathrm{H}\left(B_3 \mid A_{[2]}\right)$$

$$+\mathrm{H}\left(B_4 \mid A_{[5,6]}\right) + \mathrm{H}\left(B_5 \mid A_{4\cup 6}\right) + \mathrm{H}\left(B_6 \mid A_{[4,5]}\right) + \mathrm{H}\left(B_7 \mid A_{[8,10]}\right) + \mathrm{H}\left(B_8 \mid A_{7\cup[9,10]}\right)$$

$$+\mathrm{H}\left(B_9 \mid A_{[7,8]\cup 10}\right) + \mathrm{H}\left(B_{10} \mid A_{[7,9]}\right) + \mathrm{H}\left(B_1 \mid A_{1\cup[4,10]}, C\right) + \mathrm{H}\left(B_2 \mid A_{2\cup[4,10]}, C\right)$$

$$+\mathrm{H}\left(B_3 \mid A_{3\cup[4,10]}, C\right)+\mathrm{H}\left(B_4 \mid A_{[1,3]\cup 4\cup[7,10]}, C\right)+\mathrm{H}\left(B_5 \mid A_{[1,3]\cup 5\cup[7,10]}, C\right)$$

$$+\mathrm{H}\left(B_6 \mid A_{[1,3]\cup 6\cup[7,10]}, C\right)+\mathrm{H}\left(B_7 \mid A_{[1,7]}, C\right)+\mathrm{H}\left(B_8 \mid A_{[1,6]\cup 8}, C\right)+\mathrm{H}\left(B_9 \mid A_{[1,6]\cup 9}, C\right)$$

$$+\mathrm{H}\left(B_{10} \mid A_{[1,6]\cup 10}, C\right)+10\left[\mathrm{H}\left(C \mid A_{[10]}\right)+\sum_{i=1}^{10}\mathrm{I}\left(A_{[10]-i}; C\right)\right]+\Delta\left(A_{[10]}\right)+\nabla\left(A_{[10]}\right).$$

- *If the characteristic of* $\mathbb{F}$ *is neither* 2 *nor* 3*, then*

$$\mathrm{H}(C) \leq \frac{1}{10}\mathrm{H}\left(B_{[10]}\right)+\mathrm{H}\left(B_1 \mid A_{[2,3]}\right)+\mathrm{H}\left(B_2 \mid A_{1\cup 3}\right)+\mathrm{H}\left(B_3 \mid A_{[2]}\right)$$

$$+\mathrm{H}\left(B_4 \mid A_{[5,6]}\right)+\mathrm{H}\left(B_5 \mid A_{4\cup 6}\right)+\mathrm{H}\left(B_6 \mid A_{[4,5]}\right)+\mathrm{H}\left(B_7 \mid A_{[8,10]}\right)+\mathrm{H}\left(B_8 \mid A_{7\cup[9,10]}\right)$$

$$+\mathrm{H}\left(B_9 \mid A_{[7,8]\cup 10}\right)+\mathrm{H}\left(B_{10} \mid A_{[7,9]}\right)++\mathrm{H}\left(C \mid A_{1\cup[4,10]}, B_1\right)+\mathrm{H}\left(C \mid A_{2\cup[4,10]}, B_2\right)$$

$$+\mathrm{H}\left(C \mid A_{3\cup[4,10]}, B_3\right)+\mathrm{H}\left(C \mid A_{[1,3]\cup 4\cup[7,10]}, B_4\right)+\mathrm{H}\left(C \mid A_{[1,3]\cup 5\cup[7,10]}, B_5\right)$$

$$+\mathrm{H}\left(C \mid A_{[1,3]\cup 6\cup[7,10]}, B_6\right)+\mathrm{H}\left(C \mid A_{[1,7]}, B_7\right)+\mathrm{H}\left(C \mid A_{[1,6]\cup 8}, B_8\right)+\mathrm{H}\left(C \mid A_{[1,6]\cup 9}, B_9\right)$$

$$+\mathrm{H}\left(C \mid A_{[1,6]\cup 10}, B_{10}\right)+\mathrm{H}\left(C \mid A_{[10]}\right)+\sum_{i=1}^{10}\mathrm{I}\left(A_{[10]-i}; C\right)+\Delta\left(A_{[10]}\right)+\nabla\left(A_{[10]}\right).$$

We remark that these inequalities do not in general hold over other fields whose characteristic is different to the described characteristic. A counterexample would be in $V=\mathrm{GF}(p)^{10}$. Take the vector subspaces: $A_i=\langle e_i\rangle$, the span of each vector of the canonical basis in V; $B_i=\langle b_i\rangle$, the span of each column of the matrix B; and $C=\langle(1\cdots 1)\rangle$, the span of the vector with 1 in all entries. Then, if $p\neq 2$, the first inequality does not hold; if $p\neq 2,3$, the second inequality does not hold; if p is equal to 2 or 3, the third inequality does not hold.

Proof. To prove the inequality 1, we take a tuple of complementary vector spaces

$$\left(\bar{A}_1,\ldots,\bar{A}_{10},\bar{C}\right)$$

as obtained in Proposition 2.1.6. We remark the inequalities:

$$\mathrm{H}\left(C \mid \bar{C}\right) \leq \mathrm{H}\left(C \mid A_{[10]}\right)+\sum_{i=1}^{10}\mathrm{I}\left(A_{[10]-i}; C\right),$$

$$\mathrm{H}\left(A_i \mid \bar{A}_i\right)=\mathrm{I}\left(A_{[i-1]}; A_i\right).$$

Applying Lemma 2.1.8 several times, we get

$$\mathrm{H}\left(A_{[j,k]} \mid \bar{A}_{[j,k]}\right)=\mathrm{I}\left(A_{[1,j-1]}; A_{[j,k]}\right) \text{ for all } j,k,$$

$$\mathrm{H}\left(A_{[j,k]-i} \mid \bar{A}_{[j,k]-i}\right) \leq \mathrm{I}\left(A_{[j-1]}; A_{[j,i-1]}\right) + \mathrm{I}\left(A_{[i]}; A_{[i+1,k]}\right) \text{ for } (j,k) \in S, i \in [j,k]\,,$$

$$\mathrm{H}\left(A_{i\cup[4,10]} \mid \bar{A}_{i\cup[4,10]}\right) \leq \mathrm{I}\left(A_{i-1}; A_2\right) + \mathrm{I}\left(A_{[3]}; A_{[4,10]}\right) \text{ for } i = 1,2,$$

$$\mathrm{H}\left(A_{[4]\cup[7,10]} \mid \bar{A}_{[4]\cup[7,10]}\right) \leq \mathrm{I}\left(A_{[6]}; A_{[7,10]}\right),$$

$$\mathrm{H}\left(A_{5\cup[3]\cup[7,10]} \mid \bar{A}_{5\cup[3]\cup[7,10]}\right) \leq \mathrm{I}\left(A_{[4]}; A_5\right) + \mathrm{I}\left(A_{[6]}; A_{[7,10]}\right),$$

$$\mathrm{H}\left(A_{[3]\cup[6,10]} \mid \bar{A}_{[3]\cup[6,10]}\right) \leq \mathrm{I}\left(A_{[5]}; A_{[6,10]}\right),$$

$$\mathrm{H}\left(A_{i\cup[6]} \mid \bar{A}_{i\cup[6]}\right) \leq \mathrm{I}\left(A_{[i-1]}; A_i\right) \text{ for } i = 8,9,10.$$

One can use all these inequalities to obtain:

$$\mathrm{H}\left(A_{1\cup[4,10]} \mid \bar{A}_{1\cup[4,10]}\right) + \mathrm{H}\left(A_{2\cup[4,10]} \mid \bar{A}_{2\cup[4,10]}\right) + \mathrm{H}\left(A_{[3,10]} \mid \bar{A}_{[3,10]}\right)$$

$$+\mathrm{H}\left(A_{[1,4]\cup[7,10]} \mid \bar{A}_{[1,4]\cup[7,10]}\right) + \mathrm{H}\left(A_{[1,3]\cup5\cup[7,10]} \mid \bar{A}_{[1,3]\cup5\cup[7,10]}\right)$$

$$+\mathrm{H}\left(A_{[1,3]\cup[6,10]} \mid \bar{A}_{[1,3]\cup[6,10]}\right) + \mathrm{H}\left(A_{[1,7]} \mid \bar{A}_{[1,7]}\right) + \mathrm{H}\left(A_{[1,6]\cup8} \mid \bar{A}_{[1,6]\cup8}\right)$$

$$+\mathrm{H}\left(A_{[1,6]\cup9} \mid \bar{A}_{[1,6]\cup9}\right) + \mathrm{H}\left(A_{[1,6]\cup10} \mid \bar{A}_{[1,6]\cup10}\right) \leq \Delta\left(A_{[10]}\right),$$

$$\mathrm{H}\left(A_{[2,3]} \mid \bar{A}_{[2,3]}\right) + \mathrm{H}\left(A_{1\cup3} \mid \bar{A}_{1\cup3}\right) + \mathrm{H}\left(A_{[2]} \mid \bar{A}_{[2]}\right)$$

$$+\mathrm{H}\left(A_{[5,6]} \mid \bar{A}_{[5,6]}\right) + \mathrm{H}\left(A_{4\cup6} \mid \bar{A}_{4\cup6}\right) + \mathrm{H}\left(A_{[4,5]} \mid \bar{A}_{[4,5]}\right)$$

$$\mathrm{H}\left(A_{[8,10]} \mid \bar{A}_{[8,10]}\right) + \mathrm{H}\left(A_{7\cup[9,10]} \mid \bar{A}_{7\cup[9,10]}\right) + \mathrm{H}\left(A_{[7,8]\cup10} \mid \bar{A}_{[7,8]\cup10}\right)$$

$$+\mathrm{H}\left(A_{[7,9]} \mid \bar{A}_{[7,9]}\right) \leq \nabla\left(A_{[10]}\right).$$

Also, define

$$\bar{B}_i := B_i \cap \bar{A}_{[3]-i} \cap \left(\bar{C} + \bar{A}_{i\cup[4,10]}\right), \text{ for } i \in [3]\,;$$

$$\bar{B}_i := B_i \cap \bar{A}_{[4,6]-i} \cap \left(\bar{C} + \bar{A}_{i\cup[3]\cup[7,10]}\right), \text{ for } i \in [4,6]\,;$$

$$\bar{B}_i := B_i \cap \bar{A}_{[7,10]-i} \cap \left(\bar{C} + \bar{A}_{i\cup[6]}\right), \text{ for } i \in [7,10]\,.$$

We have the subspaces $\bar{A}_1$, …, $\bar{A}_{10}$, $\bar{B}_1$, …, $\bar{B}_{10}$, $\bar{C}$ satisfy conditions (i), (ii) of Proposition 2.1.11, and the following inequality holds

$$\mathrm{H}\left(B_1 \mid \bar{B}_1\right) \leq \mathrm{H}\left(B_1 \mid \bar{A}_{[2,3]}\right) + \mathrm{H}\left(B_1 \mid \bar{A}_{1\cup[4,10]}, \bar{C}\right)$$

$$\leq \mathrm{H}\left(B_1 \mid A_{[2,3]}\right) + \mathrm{H}\left(B_1 \mid A_{1\cup[4,10]}, C\right) + \mathrm{H}\left(A_{1\cup[4,10]} \mid \bar{A}_{1\cup[4,10]}\right)$$

$$+\mathrm{H}\left(A_{[2,3]} \mid \bar{A}_{[2,3]}\right) + \mathrm{H}\left(C \mid A_{[10]}\right) + \sum_{i=1}^{10} \mathrm{I}\left(A_{[10]-i}; C\right).$$

With an analogous argument, we can obtain upper bounds on $\mathrm{H}\left(B_i \mid \bar{B}_i\right)$ for each $i \in [2,10]$. Then, using Lemma 2.1.8, we can derive an upper bound on $\mathrm{H}\left(B_i : i \in [10] \mid \bar{B}_i : i \in [10]\right)$. The vector subspaces $\bar{A}_1$, ..., $\bar{A}_{10}$, $\bar{B}_1$, ..., $\bar{B}_{10}$, $\bar{C}$ satisfy Proposition 2.1.11 with condition 1 if the characteristic of the field $\mathbb{F}$ is 2. We have $\mathrm{H}\left(\bar{B}_{[10]}\right) \leq 8\mathrm{H}\left(\bar{C}\right)$. We can note $\mathrm{H}\left(\bar{C}\right) \leq \mathrm{I}\left(A_{[10]}; C\right)$, and derive a lower bound on $\mathrm{H}\left(\bar{B}_{[10]}\right)$ using again Lemma 2.1.8 to get the desired inequality. The inequality 2 is obtained in a similar way; and from the inequality 1, it is easy to note that the inequality 2 also holds over fields whose characteristic is 2. To prove the inequality 3, define

$$\hat{B}_i := B_i \cap \bar{A}_{[3]-i}, \text{ for } i \in [3];$$

$$\hat{B}_i := B_i \cap \bar{A}_{[4,6]-i}, \text{ for } i \in [4,6];$$

$$\hat{B}_i := B_i \cap \bar{A}_{[7,10]-i}, \text{ for } i \in [7,10];$$

$$\hat{C} := \bar{C} \cap \bigcap_{i\in[3]} \left(\hat{B}_i + \bar{A}_{i\cup[4,10]}\right) \cap \bigcap_{i\in[4,6]} \left(\hat{B}_i + \bar{A}_{i\cup[3]\cup[7,10]}\right) \cap \bigcap_{i\in[7,10]} \left(\hat{B}_i + \bar{A}_{i\cup[6]}\right).$$

We have the subspaces $\bar{A}_1$, ..., $\bar{A}_{10}$, $\hat{B}_1$, ..., $\hat{B}_{10}$, $\hat{C}$ satisfy conditions (i), (iii) of Proposition 2.1.11, and the following inequality holds

$$\mathrm{H}\left(C \mid \hat{C}\right) = \mathrm{H}\left(C \mid \bar{C}\right) + \mathrm{H}\left(\bar{C} \mid \hat{C}\right)$$

$$\leq \mathrm{H}\left(C \mid A_{[10]}\right) + \sum_{i=1}^{10} \mathrm{I}\left(A_{[10]-i}; C\right) + \mathrm{H}\left(B_1 \mid A_{[2,3]}\right) + \mathrm{H}\left(B_2 \mid A_{1\cup 3}\right) + \mathrm{H}\left(B_3 \mid A_{[2]}\right)$$

$$+\mathrm{H}\left(B_4 \mid A_{[5,6]}\right) + \mathrm{H}\left(B_5 \mid A_{4\cup 6}\right) + \mathrm{H}\left(B_6 \mid A_{[4,5]}\right) + \mathrm{H}\left(B_7 \mid A_{[8,10]}\right) + \mathrm{H}\left(B_8 \mid A_{7\cup[9,10]}\right)$$

$$+\mathrm{H}\left(B_9 \mid A_{[7,8]\cup 10}\right) + \mathrm{H}\left(B_{10} \mid A_{[7,9]}\right) + +\mathrm{H}\left(C \mid A_{1\cup[4,10]}, B_1\right) + \mathrm{H}\left(C \mid A_{2\cup[4,10]}, B_2\right)$$

$$+\mathrm{H}\left(C \mid A_{3\cup[4,10]}, B_3\right) + \mathrm{H}\left(C \mid A_{[1,3]\cup 4\cup[7,10]}, B_4\right) + \mathrm{H}\left(C \mid A_{[1,3]\cup 5\cup[7,10]}, B_5\right)$$

$$+\mathrm{H}\left(C \mid A_{[1,3]\cup 6\cup[7,10]}, B_6\right) + \mathrm{H}\left(C \mid A_{[1,7]}, B_7\right) + \mathrm{H}\left(C \mid A_{[1,6]\cup 8}, B_8\right) + \mathrm{H}\left(C \mid A_{[1,6]\cup 9}, B_9\right)$$

$$+\mathrm{H}\left(C \mid A_{[1,6]\cup 10}, B_{10}\right) + \Delta\left(A_{[10]}\right) + \nabla\left(A_{[10]}\right).$$

So, the vector subspaces $\bar{A}_1$, ..., $\bar{A}_{10}$, $\hat{B}_1$, ..., $\hat{B}_{10}$, $\hat{C}$ satisfy Proposition 2.1.11 with condition 3 if the characteristic of the field $\mathbb{F}$ is neither 2 nor 3. We have $10\mathrm{H}\left(\hat{C}\right) \leq \mathrm{H}\left(\hat{B}_{[10]}\right)$. We can note $\mathrm{H}\left(\hat{B}_{[10]}\right) \leq \mathrm{H}\left(B_{[10]}\right)$ and derive a lower bound on $\mathrm{H}\left(\hat{C}\right)$ from the upper bound on $\mathrm{H}\left(C \mid \hat{C}\right)$ to get the desired inequality. □

2.1.2 Producing inequalities

In this section, we show the theorem that produces characteristic-dependent linear rank inequalities using suitable binary matrices. In order to gain a better understanding, the theorem is divided in several lemmas and propositions; we are going to show them in three sub-subsections or steps as follow:

- Finding an equation: We specify the form of the matrices that can produce inequalities.

- Conditional characteristic-dependent linear rank inequalities: We describe linear inequalities that depend on the characteristic and some conditions of the involved linear random variables using as a guide the matrices described in previous step.

- Characteristic-dependent linear rank inequalities: We finally produce inequalities.

2.1.2.1 Finding an equation

Consider any binary $n \times m$ matrix B, with columns denoted by b_i. Let π_{b_i} be the I_i-projection of $V = A_1 \oplus \cdots \oplus A_n$, where

$$I_i := \bar{b}_i = \left\{ j \in [n] : b_i^j = 1 \right\}.$$

Take

$$b_{I_i} := \sum_j b_{I_i}^j e_j \in V,$$

where $(e_j)_j$ is the canonical basis in V; and

$$b_{I_i}^j := \begin{cases} 1 & \text{if } e_j \in A_k \text{ for some } k \text{ such that } b_k = 1. \\ 0 & \text{in otherwise.} \end{cases}$$

If $x = \sum_j x_j e_j$, then we have

$$\pi_{b_i}(x) = b_{I_i} \cdot x := \sum_j b_{I_i}^j x_j e_j.$$

We have the following proposition.

Lemma 2.1.13. *Let $V = A_1 \oplus \cdots \oplus A_n$, $A_i \neq O$, and let B be a $n \times m$ binary matrix. For all i and I, we have $b_i = \sum_{j \in I} \alpha_j b_j$ if and only if $\pi_{b_i} = \sum_{j \in I} \alpha_j \pi_{b_j}$.*

Proof. We note $b_i = \sum_{j\in I}\alpha_j b_j$ if and only if $b_{I_i} = \sum_{j\in I}\alpha_j b_{I_j}$. Now, let $b_i = \sum_{j\in I}\alpha_j b_j$. For $x \in V$,

$$\sum_{j\in I}\alpha_j \pi_{b_j}(x) = \sum_{j\in I}\alpha_j \left(b_{I_j}\cdot x\right) = \sum_{j\in I}\left(\alpha_j b_{I_j}\cdot x\right)$$

$$= \left(\sum_{j\in I}\alpha_j b_{I_j}\right)\cdot x = b_{I_i}\cdot x = \pi_{b_i}(x).$$

The other implication is obtained from

$$\pi_{b_i}(1\cdots 1) = \sum_{j\in I}\alpha_j \pi_{b_j}(1\cdots 1).$$

□

Example 2.1.14. Take

$$B = \begin{array}{c} \begin{matrix} b_1 & b_2 & b_3 \end{matrix} \\ \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \end{array}.$$

In $V = \mathrm{GF}(2)^5$, we define $A_1 = \langle e_1, e_4\rangle$, $A_2 = \langle e_2, e_5\rangle$, $A_3 = \langle e_3\rangle$. We have

$$b_{I_1} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}, b_{I_2} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, b_{I_3} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}.$$

One can check that $b_1 = b_2 + b_3$ and $b_{I_1} = b_{I_2} + b_{I_3}$.

Theorem 2.1.15. *Let $(A_1, \ldots, A_n, C)$ be a tuple of complementary vector subspaces in V over $\mathbb{F}$ with $C \neq O$, and let B be a $n \times m$ binary matrix with columns denoted by b_i. We have $\{b_i\}_{i\in I}$ is an independent set if and only if $\sum_{i\in I}\pi_{b_i}(C)$ is a direct sum.*

Proof. We suppose that $\{b_i\}_{i\in I}$ is a dependent set and prove that $\sum_{i\in I}\pi_{b_i}(C)$ is not a direct sum. There exists $k \in I$ such that $b_k = \sum_{i\in I-k}\alpha_i b_i$ for some $\alpha_i \in \mathbb{F}$ not all zero. By Lemma 2.1.13, we get $\pi_{b_k}(c) = \sum_{i\in I-k}\alpha_i \pi_{b_i}(c)$ for some $c \in C - O$. In other words, $\sum_{i\in I}\pi_{b_i}(C)$ is not a direct sum. Reciprocally, we suppose that $\sum_{i\in I}\pi_{b_i}(C)$ is not a direct sum, and we prove that $\{b_i\}_{i\in I}$ is a dependent set. There exist $c_1, \ldots, c_{|I|} \in C$ not all zero such that $\sum_{i\in I}\pi_{b_i}(c_i) = O$.

Thus,

$$O = \sum_{i \in I} (b_{I_i} \cdot c_i) = \sum_{i \in I} \left(\sum_j b_{I_i}^j c_i^j e_j \right) = \sum_j \left(\sum_{i \in I} b_{I_i}^j c_i^j \right) e_j,$$

which implies that

$$\sum_{i \in I} b_{I_i}^j c_i^j = 0,$$

for all j. By Lemma 2.1.13,

$$\sum_{i \in I} b_i c_i^j = 0,$$

for all j. Since not all c_i is zero, we obtain that $\{b_i\}_{i \in I}$ is a dependent set. □

We have the following statement.

Corollary 2.1.16. *Let $B = (B^i) = (e_{S_i})$ be a $n \times m$ binary matrix over a finite field $\mathbb{F}$, $m \leq n$ and $t_i \geq 2$, for $i = 1, \ldots, s$, $m > m_s > \cdots > m_i > \cdots > m_1 \geq 1$ integers. We suppose that* $\mathrm{rank}\,(B) = m_i$ *if* $\mathrm{char}\,(\mathbb{F})$ *divides t_i, and* $\mathrm{rank}\,(B) = m$ *in other cases. Then, for any tuple of complementary vector subspaces $(A_1, \cdots, A_n, C)$ holds*

$$\mathrm{H}\left(\pi_{S_i}(C) : i \in [m]\right) = \begin{cases} m_1 \mathrm{H}(C) & \text{if } \mathrm{char}\,(\mathbb{F}) \mid t_1. \\ \quad \vdots & \quad \vdots \\ m_s \mathrm{H}(C) & \text{if } \mathrm{char}\,(\mathbb{F}) \mid t_s. \\ m \mathrm{H}(C) & \text{if } \mathrm{char}\,(\mathbb{F}) \nmid t = \prod_i t_i. \end{cases}$$

Proof. In case $\mathrm{char}\,(\mathbb{F})$ does not divide t, $\sum_{i \in [m]} \pi_{b_i}(C)$ is a direct sum by Theorem 2.1.15. Then, we have

$$\mathrm{H}\left(\pi_{S_i}(C) : i \in [m]\right) = \sum_{i \in [m]} \mathrm{H}\left(\pi_{S_i}(C)\right) = m\mathrm{H}(C) \text{ [from Proposition 2.1.4].}$$

Fixed k, we now suppose that $\mathrm{rank} B = m_k$ if $\mathrm{char}\,(\mathbb{F})$ divides t_k. There exists $I \subsetneq [m]$ such that the rank of the submatrix B_I of B is m_k. Then,

$$\begin{aligned} \mathrm{H}\left(\pi_{S_i}(C) : i \in [m]\right) &= \mathrm{H}\left(\pi_{S_i}(C) : i \in I\right) \text{ [from Theorem 2.1.15]} \\ &= \sum_{i \in I} \mathrm{H}\left(\pi_{S_i}(C)\right) \text{ [from Theorem 2.1.15]} \\ &= m_k \mathrm{H}(C) \text{ [from Proposition 2.1.4].} \end{aligned}$$

□

2.1.2.2 Conditional characteristic-dependent linear rank inequalities

Definition 2.1.17. For a binary matrix B, we denote $B = (B^i) = (e_{S_i})$, with $S_i = \left\{j : B_{(j,i)} = 1\right\}$, and we define the sets:

$$\mathcal{B}' := \{e_{S_i} : 1 < |S_i| < n\},$$

$$\mathcal{B}'' := \{e_{S_i} : |S_i| = 1\},$$

$$\mathcal{B}''' := \begin{cases} \{C\} & \text{if there exists } e_{S_i} \text{ in } B \text{ such that } |S_i| = n. \\ \emptyset & \text{in other case.} \end{cases}$$

We assume without lost of generality that $e_{S_i} = e_i$ if $|S_i| = 1$.

We introduce the following notation:

$$[e_n, e_m] = \{e_i : n \leq i \leq m\},$$

$$[e_n, e_m) = \{e_i : n \leq i < m\},$$

$$[e_n] := [e_1, e_n] = \{e_i : i \leq n\}.$$

From now on, we consider vector subspaces indexed by the columns of some matrix B.

The described conditions in the following two lemmas are derived from the dependency relationships of the columns of B.

Proposition 2.1.18. *For each t_k, let $\mathbb{F}$ be a finite field such that $\mathrm{char}(\mathbb{F})$ divides t_k. For any vector subspaces $A_{e_1}, \ldots, A_{e_n}$, $B_{e_{S_{j_1}}}, \ldots, B_{e_{S_{j_{|\mathcal{B}'|}}}}$ and C of a finite dimensional vector space V over $\mathbb{F}$, such that $(A_{e_1}, \ldots, A_{e_n}, C)$ is a tuple of complementary vector subspaces and*

(i) $A_{e_i} \leq A_{[e_n]-e_i} \oplus C$ for i such that $e_i \in \mathcal{B}''$,

(ii) $B_{e_{S_i}} \leq \bigoplus_{j \in S_i} A_{e_j}$ for $e_{S_i} \in \mathcal{B}'$,

(iii) $B_{e_{S_i}} \leq \bigoplus_{j \notin S_i} A_{e_j} \oplus C$ for $e_{S_i} \in \mathcal{B}'$.

We have

$$\mathrm{H}\left(A_{e_i}, B_{e_{S_j}}, C : e_{S_j} \in \mathcal{B}', e_i \in \mathcal{B}'', C \in \mathcal{B}'''\right) \leq m_k \mathrm{H}(C).$$

Proof. Since the characteristic divides t_k, applying Corollary 2.1.16, we get

$$\mathrm{H}(\pi_{S_i}(C) : i \in [m]) = m_k \mathrm{H}(C). \tag{2.1.1}$$

On the other hand, we have

$$\pi_{S_i}(C) = \left(C + \bigoplus_{j \notin S_i} A_{e_j}\right) \cap \left(\bigoplus_{j \in S_i} A_{e_j}\right), \text{ for all } i. \tag{2.1.2}$$

In effect, let $v \in C$ such that $v = \sum_i v_i$, where $v_i \in A_i$, and fixed $j \in [n+1]$. Noting that $\pi_{S_j}(v) = \sum_{i \in S_j} v_i = v - \sum_{i \notin S_j} v_i$, we get

$$\pi_{S_j}(v) \in \left(C + \bigoplus_{i \notin S_j} A_{e_i}\right) \cap \left(\bigoplus_{i \in S_j} A_{e_i}\right).$$

To prove the other containment, let $u \in \left(C + \bigoplus_{i \notin S_j} A_{e_i}\right) \cap \left(\bigoplus_{i \in S_j} A_{e_i}\right)$. Then, there exist $v \in C$ and $v_i \in A_i$, for all i, such that $u = v - \sum_{i \notin S_j} v_i = \sum_{i \in S_j} v_i$. Thus $v = \sum_i v_i$ and $u = \pi_{S_i}(v) \in \pi_{S_i}(C)$. It follows that equality 2.1.2 is true. Therefore, using hypothesis (ii), we have that

$$A_{e_i} \leq \pi_{S_i}(C),\ e_i \in \mathcal{B}\text{" [from hypothesis (i)]},$$

$$B_{e_{S_i}} \leq \pi_{S_i}(C),\ e_{S_i} \in \mathcal{B}\text{' [from hypothesis (ii) and (iii)]},$$

which implies

$$\left(\sum_{e_i \in \mathcal{B}''} A_{e_i}\right) + \left(\sum_{e_{S_j} \in \mathcal{B}'} B_k\right) + (C)_{C \in \mathcal{B}'''} \leq \sum_i \pi_{S_i}(C) \text{ [also, note that } C \leq \pi_{1\cdots 1}(C)].$$

From equation (2.1.1), we get $\mathrm{H}\left(A_{e_i}, B_{e_{S_j}}, C : e_{S_j} \in \mathcal{B}', e_i \in \mathcal{B}'', C \in \mathcal{B}'''\right) \leq m_k \mathrm{H}(C)$. □

Proposition 2.1.19. *Let $\mathbb{F}$ be a finite field such that $\mathrm{char}(\mathbb{F})$ does not divide $t = \prod_i t_i$. For any vector subspaces $A_{e_1}, \ldots, A_{e_n}$, $B_{e_{S_{j_1}}}, \ldots, B_{e_{S_{j_{|\mathcal{B}'|}}}}$ and C of a finite dimensional vector space V over $\mathbb{F}$, such that $(A_{e_1}, \ldots, A_{e_n}, C)$ is a tuple of complementary vector subspaces and*

(i) $B_{e_{S_i}} \leq \bigoplus_{j \in S_i} A_{e_j}$ for $e_{S_i} \in \mathcal{B}'$.

(ii) $C \leq \bigoplus_{j \notin S_i} A_{e_j} + B_{e_{S_i}}$ for $e_{S_i} \in \mathcal{B}'$.

We have

$$m\mathrm{H}(C) \leq H\left(A_{e_i}, B_{e_{S_j}}, C : e_{S_j} \in \mathcal{B}', e_i \in \mathcal{B}'', C \in \mathcal{B}'''\right).$$

Proof. Since the characteristic does not divide t, applying Corollary 2.1.16, we get

$$\mathrm{H}(\pi_{S_i}(C) : i \in [m]) = m\mathrm{H}(C). \tag{2.1.3}$$

On the other hand, $\pi_{S_k}(C) \leq B_k$ for all k such that $e_{S_k} \in \mathcal{B}'$; $\pi_{S_k}(C) \leq A_{e_k}$ for all k such that $e_{S_k} \in \mathcal{B}''$; $\pi_{1\cdots 1}(C) \leq C$ if $C \in \mathcal{B}'''$. The last two affirmation are trivial by definition of projection. To prove the first affirmation, fixed $k \in [m]$ and let $v = \sum_i v_i \in C$, where $v_i \in A_i$. By condition (ii), there exist $a_k^i \in A_{e_k}$, $i \in [m] - S_k$ and $b_k \in B_{e_{S_k}}$ such that $v = \sum_{i \notin S_k} a_k^i + b_k$. By condition (i), there exists $a_i \in A_{e_i}$, for each $i \in S_k$, such that $b_k = \sum_{i \in S_k} a_i$. Then, $v = \sum_i v_i = \sum_{i \in S_k} a_i + \sum_{i \notin S_k} a_k^i$, but v has unique writing in terms of A_i, in particular, $a_i = v_i$, for each $i \in S_k$. We get

$$\pi_{S_k}(v) = \sum_{i \in S_k} v_i = b_k \in B_{e_{S_k}}.$$

In other words,

$$\pi_{S_k}(C) \leq B_{e_{S_k}}.$$

Hence,

$$\sum_i \pi_{S_i}(C) \leq \left(\sum_{e_i \in \mathcal{B}''} A_{e_i} \right) + \left(\sum_{e_{S_j} \in \mathcal{B}'} B_{e_{S_i}}. \right) + (C)_{\text{in case } C \in \mathcal{B}'''}$$

Therefore, using equation (2.1.3) we get,

$$m\mathrm{H}(C) \leq \mathrm{H}\left(A_{e_i}, B_{e_{S_j}}, C : e_{S_j} \in \mathcal{B}', e_i \in \mathcal{B}'', C \in \mathcal{B}''' \right).$$

□

2.1.2.3 Characteristic-dependent linear rank inequalities

We now show three lemmas that will help to the demonstration of the main theorem. We remark that for any $A_{e_1}, \ldots, A_{e_n}$ and C vector subspaces of a vector spaces V, by Proposition 2.1.6, there exists a tuple $\left(A'_{e_1}, \ldots, A'_{e_n}, \bar{C} \right)$ of complementary vector subspaces in $A_{e_1} + \ldots + A_{e_n} \leq V$ which holds:

$$\mathrm{H}\left(A_{e_k} \mid A'_{e_k} \right) = \mathrm{I}\left(A_{[e_{k-1}]}; A_{e_k} \right), \text{ for all } k, \tag{2.1.4}$$

$$\mathrm{H}\left(C \mid \bar{C} \right) \leq \nabla(C) := \mathrm{H}\left(C \mid A_{[e_n]} \right) + \sum_{e_i \in [e_n]} \mathrm{I}\left(A_{[e_n]-e_i}; C \right). \tag{2.1.5}$$

Additionally, for $T \subseteq [e_n]$, it is straightforward to take some elements $e_{k_1}, \ldots, e_{k_l}$ with

$$k_1 \leq k_2 \leq \cdots \leq k_l$$

such that it is possible to built a partition in intervals $\left[e_{k_i}, e_{k_j}\right]$, with maximum length, of T. Using Lemma 2.1.8, we get

$$\mathrm{H}\left(A_e : e \in T \mid A'_e : e \in T\right) \leq \nabla\left(A_e : e \in T\right)$$

$$:= \mathrm{I}\left(A_{\left[e_1, e_{k_1}\right)}; A_{\left[e_{k_1}, e_{k_2}\right]}\right) + \cdots + \mathrm{I}\left(A_{\left[e_1, e_{k_1-1}\right)}; A_{\left[e_{k_{1-1}}, e_{k_l}\right]}\right). \tag{2.1.6}$$

Lemma 2.1.20. *Let $A_{e_1}, \ldots, A_{e_n}$ and C be vector subspaces of a vector spaces V. Define*

$$\bar{A}_{e_k} := A'_{e_k} \cap \left(\bar{C} + \bigoplus_{e_i \notin \mathcal{B}''} A'_{e_i} + \bigoplus_{e_i \in \mathcal{B}'', i<k} \bar{A}_{e_i} + \bigoplus_{e_i \in \mathcal{B}'', i>k} A'_{e_i}\right), \text{ for } e_k \in \mathcal{B}''.$$

$$\bar{A}_{e_k} := A'_{e_k}, \text{ for } e_k \notin \mathcal{B}''.$$

Then, $\left(\bar{A}_{e_1}, \ldots, \bar{A}_{e_n}, \bar{C}\right)$ is a tuple of complementary vector subspaces that satisfies (i) in Lemma 2.1.18 and

$$\mathrm{H}\left(\bar{A}_{e_k}\right) = \mathrm{H}\left(\bar{C}\right), \text{ for } e_k \in \mathcal{B}'',$$

$$\mathrm{H}\left(\bar{A}_{e_k}\right) = \mathrm{H}\left(A_{e_k} \mid A_{[e_{k-1}]}\right), \text{ for } e_k \in \mathcal{B}',$$

$$\mathrm{H}\left(A_{e_k} \mid \bar{A}_{e_k}\right) \leq \mathrm{H}\left(A_{e_k}\right) - \mathrm{H}\left(C\right) + \nabla\left(C\right), \text{ for } e_k \in \mathcal{B}''. \tag{2.1.7}$$

Proof. We obviously have

$$\bar{A}_{e_k} \leq \bar{C} + \bigoplus_{e_i \notin \mathcal{B}''} A'_{e_i} + \bigoplus_{e_i \in \mathcal{B}'', i<k} \bar{A}_{e_i} + \bigoplus_{e_i \in \mathcal{B}'', i>k} A'_{e_i}.$$

Now, for any k such that $e_k \in \mathcal{B}''$, we have

$$\bar{C} \leq \bigoplus_{e_i \notin \mathcal{B}''} A'_{e_i} + \bigoplus_{e_i \in \mathcal{B}'', i \leq k} \bar{A}_{e_i} + \bigoplus_{e_i \in \mathcal{B}'', i>k} A'_{e_i}. \tag{2.1.8}$$

In effect, we show case $k = l := \min\left\{i : e_i \in \mathcal{B}''\right\}$, i.e. we have to show that

$$\bar{C} \leq \left(\bigoplus_{i \neq l'} A'_{e_i}\right) + \bar{A}_{e_l}.$$

The general case is proved by induction, we omit the proof. We note case $\bar{C} = O$ is trivial. So, we suppose that there exist $c \in \bar{C} - O$, then from Corollary 2.1.5, $c = \sum\limits_i a_i$ for some $a_i \in A'_{e_i} - O$. Thus,

$$a_l = c - \sum_{i \neq l} a_i \in \left[\bar{C} \oplus \left(\bigoplus_{i \neq l'} A'_{e_i}\right)\right] \cap A'_{e_l}.$$

Therefore, $a_l \in \bar{A}_{e_l}$, which implies $c \in \left(\bigoplus_{i\neq l'} A'_{e_i}\right) + \bar{A}_{e_l}$. So, (2.1.8) is true. Taking $k = \max\{i : e_i \in \mathcal{B}''\}$, we obtain that $\bar{C} \leq \bigoplus \bar{A}_{e_i}$. Hence, the described tuple is a tuple of complementary vector subspaces that satisfies (i) in Lemma 2.1.18. We also have the equation:

$$\mathrm{H}\left(\bar{A}_{e_k}\right) = \mathrm{I}\left(A'_{e_k}; \bar{C}, \bigoplus_{e_i\notin\mathcal{B}''} A'_{e_i}, \bigoplus_{e_i\in\mathcal{B}'',i<k} \bar{A}_{e_i}, \bigoplus_{e_i\in\mathcal{B}'',i>k} A'_{e_i}\right)$$

$$= \mathrm{H}\left(A'_{e_k}\right) - \mathrm{H}\left(\bigoplus_{e_i\notin\mathcal{B}''} A'_{e_i}, \bigoplus_{e_i\in\mathcal{B}'',i<k} \bar{A}_{e_i}, \bigoplus_{e_i\in\mathcal{B}'',i\geq k} A'_{e_i}\right) + \mathrm{H}\left(\bar{C}, \bigoplus_{e_i\notin\mathcal{B}''} A'_{e_i}, \bigoplus_{e_i\in\mathcal{B}'',i<k} \bar{A}_{e_i}, \bigoplus_{e_i\in\mathcal{B}'',i>k} A'_{e_i}\right)$$

[from definition of mutual information and (2.1.8)]

$$= \mathrm{H}\left(\bar{C}\right). \qquad \text{[definition of complementary subspaces]}$$

This can also be used to obtain the described upper bound on $\mathrm{H}\left(A_{e_k} \mid \bar{A}_{e_k}\right)$. □

Lemma 2.1.21. *Let $A_{e_1}, \ldots, A_{e_n}$, $B_{e_{S_{j_1}}}, \ldots, B_{e_{S_{j_{|\mathcal{B}'|}}}}$ and C be vector subspaces of a vector spaces V. For each $e_{S_k} \in \mathcal{B}'$, we define*

$$\bar{B}_{e_{S_k}} := B_{e_{S_k}} \cap \left(\bigoplus_{e_i\in S_k} \bar{A}_{e_i}\right) \cap \left(\bigoplus_{e_i\notin S_k} \bar{A}_{e_i} \oplus \bar{C}\right).$$

We have the subspaces $\bar{A}_{e_1}, \ldots, \bar{A}_{e_n}$, $\bar{B}_{e_{S_{j_1}}}, \ldots, \bar{B}_{e_{S_{j_{|\mathcal{B}'|}}}}$ and $\bar{C}$ satisfy hypothesis in Lemma 2.1.18 and

$$\mathrm{H}\left(B_{e_{S_k}} \mid \bar{B}_{e_{S_k}}\right) \leq \mathrm{H}\left(B_{e_{S_k}} \mid A_{e_i} : i \in S_k\right) + \mathrm{H}\left(B_{e_{S_k}} \mid A_{e_i}, C : i \notin S_k\right) + \sum_{e_i\in\mathcal{B}''} \mathrm{H}\left(A_{e_i}\right)$$

$$+\nabla\left(A_{e_i} : i \in S_k, e_i \notin \mathcal{B}''\right) + \nabla\left(A_{e_i} : i \notin S_k, e_i \notin \mathcal{B}''\right) + \left(|\mathcal{B}''| + 1\right)\nabla\left(C\right) - |\mathcal{B}''|\,\mathrm{H}\left(C\right)$$

Proof. The conditions in Lemma 2.1.18 are obviously true. To prove the inequality, we have

$$\mathrm{H}\left(B_{e_{S_k}} \mid \bar{B}_{e_{S_k}}\right) \leq \mathrm{H}\left(B_{e_{S_k}} \mid \left(\bigoplus_{i\in S_k} \bar{A}_{e_i}\right) \cap B_{e_{S_k}}\right) + \mathrm{H}\left(B_{e_{S_k}} \mid \left[\bigoplus_{i\notin S_k} \bar{A}_{e_i} \oplus \bar{C}\right] \cap B_{e_{S_k}}\right)$$

$$= \mathrm{H}\left(B_{e_{S_k}} \mid \left(\bigoplus_{i\in S_k} A_{e_i}\right) \cap B_{e_{S_k}}\right) + \mathrm{H}\left(B_{e_{S_k}} \mid \left[\bigoplus_{i\notin S_k} A_{e_i} \oplus C\right] \cap B_{e_{S_k}}\right)$$

$$+\mathrm{H}\left(\left(\sum_{i\in S_k} A_{e_i}\right) \cap B_{e_{S_k}} \mid \left(\bigoplus_{i\in S_k} \bar{A}_{e_i}\right) \cap B_{e_{S_k}}\right)$$

$$+\mathrm{H}\left(\left[\sum_{i\notin S_k} A_{e_i}\oplus C\right]\cap B_{e_{S_k}} \mid \left[\bigoplus_{i\notin S_k}\bar{A}_{e_i}\oplus\bar{C}\right]\cap B_{e_{S_k}}\right)$$

$$\leq \mathrm{H}\left(B_{e_{S_k}} \mid A_{e_i} : i\in S_k\right)+\mathrm{H}\left(B_{e_{S_k}} \mid C, A_{e_i} : i\notin S_k\right)$$

$$+\mathrm{H}\left(\sum_{i\in S_k, e_i\in\mathcal{B}''} A_{e_i} \mid \bigoplus_{i\in S_k, e_i\in\mathcal{B}''}\bar{A}_{e_i}\right)+\mathrm{H}\left(\sum_{i\in S_k, e_i\notin\mathcal{B}''} A_{e_i} \mid \bigoplus_{i\in S_k, e_i\notin\mathcal{B}''} A'_{e_i}\right)+$$

$$\mathrm{H}\left(\sum_{i\notin S_k, e_i\in\mathcal{B}''} A_{e_i} \mid \bigoplus_{i\notin S_k, e_i\in\mathcal{B}''}\bar{A}_{e_i}\right)+\mathrm{H}\left(\sum_{i\notin S_k, e_i\notin\mathcal{B}''} A_{e_i} \mid \bigoplus_{i\notin S_k, e_i\notin\mathcal{B}''} A'_{e_i}\right)+\mathrm{H}\left(C \mid \bar{C}\right)$$

$$\leq \mathrm{H}\left(B_{e_{S_k}} \mid A_{e_i} : i\in S_k\right)+\mathrm{H}\left(B_{e_{S_k}} \mid A_{e_i}, C : i\notin S_k\right)+\sum_{i\in S_k, e_i\in\mathcal{B}''}\mathrm{H}\left(A_{e_i}\right)$$

$$+\left|\{e_i\in\mathcal{B}'' : i\in S_k\}\right|\left(\nabla\left(C\right)-\mathrm{H}\left(C\right)\right)+\nabla\left(A_{e_i} : i\in S_k, e_i\notin\mathcal{B}''\right)+\sum_{i\notin S_k, e_i\in\mathcal{B}''}\mathrm{H}\left(A_{e_i}\right)$$

$$+\left|\{e_i\in\mathcal{B}'' : i\notin S_k\}\right|\left(\nabla\left(C\right)-\mathrm{H}\left(C\right)\right)+\nabla\left(A_{e_i} : i\notin S_k, e_i\notin\mathcal{B}''\right)+\nabla\left(C\right)$$

[from Lemmas 2.1.8 and 2.1.9, inequalities (2.1.6) and (2.1.7)].

$$=\mathrm{H}\left(B_{e_{S_k}} \mid A_{e_i} : i\in S_k\right)+\mathrm{H}\left(B_{e_{S_k}} \mid A_{e_i}, C : i\notin S_k\right)+\sum_{e_i\in\mathcal{B}''}\mathrm{H}\left(A_{e_i}\right)$$

$$+\left(\left|\mathcal{B}''\right|+1\right)\nabla\left(C\right)-\left|\mathcal{B}''\right|\mathrm{H}\left(C\right)+\nabla\left(A_{e_i} : i\in S_k, e_i\notin\mathcal{B}''\right)+\nabla\left(A_{e_i} : i\notin S_k, e_i\notin\mathcal{B}''\right)$$

□

Lemma 2.1.22. *Let $A_{e_1},\ldots,A_{e_n}$, $B_{e_{S_{j_1}}},\ldots,B_{e_{S_{j_{|\mathcal{B}'|}}}}$ and C be vector subspaces of a vector spaces V. For each $e_{S_k}\in\mathcal{B}'$, we define $\hat{B}_{e_{S_k}} := B_{e_{S_k}}\cap\bigoplus_{j\in S_k} A'_{e_j}$ and*

$$\hat{C} := \bar{C}\bigcap_{e_{S_k}}\left(\bigoplus_{j\notin S_i} A'_{e_j}+\hat{B}_{e_{S_k}}\right).$$

We have $A'_{e_1},\ldots,A'_{e_n}$, $\hat{B}_{e_{S_{j_1}}},\ldots,\hat{B}_{e_{S_{j_{|\mathcal{B}'|}}}}$ and $\hat{C}$ satisfy hypothesis in Lemma 2.1.19 and

$$\mathrm{H}\left(B_{e_{S_k}} \mid \hat{B}_{e_{S_k}}\right)\leq \mathrm{H}\left(B_{e_{S_k}} \mid A_{e_i} : i\in S_k\right)+\nabla\left(A_{e_i} : i\in S_k\right), \tag{2.1.9}$$

$$\mathrm{H}\left(C \mid \hat{C}\right)\leq \nabla\left(C\right)+\sum_{e_{S_k}\in\mathcal{B}'}\left[\mathrm{H}\left(C \mid A_{e_i}, B_{S_k} : i\notin S_k\right)+\mathrm{H}\left(B_{e_{S_k}} \mid A_{e_i} : i\in S_k\right)\right]$$

$$+\sum_{e_{S_k}\in\mathcal{B}'}\left[\nabla\left(A_{e_i} : i\notin S_k\right)+\nabla\left(A_{e_i} : i\in S_k\right)\right]. \tag{2.1.10}$$

Proof. By definition, we remark that $\left(A'_{e_1},\ldots,A'_{e_n},\hat{C}\right)$ is also a tuple of complementary vec-

tor subspaces and the other conditions in 2.1.19 are also true. We only show last inequality:

$$\mathrm{H}\left(C \mid \hat{C}\right) \leq \mathrm{H}\left(C \mid \bar{C}\right) + \sum_{e_{S_k} \in \mathcal{B}'} \mathrm{H}\left(C \mid C \cap \left[\bigoplus_{i \notin S_k} A'_{e_i} + \hat{B}_{e_{S_k}}\right]\right)$$

$$= \mathrm{H}\left(C \mid \bar{C}\right) + \sum_{e_{S_k} \in \mathcal{B}'} \mathrm{H}\left(C \mid C \cap \left[\bigoplus_{i \notin S_k} A_{e_i} + B_{e_{S_k}}\right]\right)$$

$$+ \sum_{e_{S_k} \in \mathcal{B}'} \mathrm{H}\left(C \cap \left[\sum_{i \notin S_k} A_{e_i} + B_{e_{S_k}}\right] \mid C \cap \left[\bigoplus_{i \notin S_k} A'_{e_i} + \hat{B}_{e_{S_k}}\right]\right)$$

$$\leq \mathrm{H}\left(C \mid \bar{C}\right) + \sum_{e_{S_k} \in \mathcal{B}'} \mathrm{H}\left(C \mid \bigoplus_{i \notin S_k} A_{e_i} + B_{e_{S_k}}\right) + \sum_{e_{S_k} \in \mathcal{B}'} \mathrm{H}\left(\sum_{i \notin S_k} A_{e_i} \mid \bigoplus_{i \notin S_k} A'_{e_i}\right)$$

$$+ \sum_{e_{S_k} \in \mathcal{B}'} \mathrm{H}\left(B_{e_{S_k}} \mid \hat{B}_{e_{S_k}}\right) \text{ [from Lemmas 2.1.8 and 2.1.9, and inequality (2.1.9)]}$$

$$\leq \nabla(C) + \sum_{e_{S_k} \in \mathcal{B}'} \left[\mathrm{H}\left(C \mid A_{e_i}, B_{S_k} : i \notin S_k\right) + \mathrm{H}\left(B_{e_{S_k}} \mid A_{e_i} : i \in S_k\right)\right]$$

$$+ \sum_{e_{S_k} \in \mathcal{B}'} \left[\nabla\left(A_{e_i} : i \notin S_k\right) + \nabla\left(A_{e_i} : i \in S_k\right)\right] \text{ [from (2.1.6)]}$$

□

The following theorem finally shows our first method for producing characteristic-dependent linear rank inequalities.

Theorem 2.1.23. *Let $B = (B^i) = (e_{S_i})$ be a $n \times m$ binary matrix over a finite field $\mathbb{F}$, $m \leq n$ and $t_i \geq 2$, $m > m_s > \cdots > m_i > \cdots m_1 \geq 1$ integers. We suppose that $rank(B) = m_i$ if $char(\mathbb{F})$ divides t_i, and $rank(B) = m$ in other cases. Let $A_{e_1}, \ldots, A_{e_n}$, $B_{e_{S_{j_1}}}, \ldots, B_{e_{S_{j_{|\mathcal{B}'|}}}}$ and C be vector subspaces of a finite dimensional vector space V over a finite field $\mathbb{F}$. Then*

(i) *For each $k = 1, \ldots, s$, the following inequality is a characteristic-dependent linear rank inequality over fields whose characteristic divides $\prod_{i \leq k} t_i$,*

$$\mathrm{H}\left(A_{e_j}, B_{e_{S_i}}, C : e_{S_i} \in \mathcal{B}', e_j \in \mathcal{B}'', C \in \mathcal{B}'''\right) + \left(|\mathcal{B}''|\,|\mathcal{B}'| + |\mathcal{B}''|\right) \mathrm{H}(C) \leq m_k \mathrm{I}\left(A_{[e_n]}; C\right)$$

$$+ \sum_{e_{S_k} \in \mathcal{B}'} \left[\mathrm{H}\left(B_{e_{S_k}} \mid A_{e_i}, C : i \notin S_k\right) + \mathrm{H}\left(B_{e_{S_k}} \mid A_{e_i} : i \in S_k\right)\right] + \left(|\mathcal{B}'| + 1\right) \sum_{e_i \in \mathcal{B}''} \mathrm{H}\left(A_{e_i}\right)$$

$$+ \left(|\mathcal{B}''|\,|\mathcal{B}'| + |\mathcal{B}'''| + |\mathcal{B}''| + |\mathcal{B}'|\right) \left[\mathrm{H}\left(C \mid A_{[e_n]}\right) + \sum_{e_i \in [e_n]} \mathrm{I}\left(A_{[e_n]-e_i}; C\right)\right]$$

$$+\sum_{e_{S_k}\in\mathcal{B}'}\left[\nabla\left(A_{e_i}:i\in S_k,e_i\notin\mathcal{B}''\right)+\nabla\left(A_{e_i}:i\notin S_k,e_i\notin\mathcal{B}''\right)\right].$$

(ii) *The following inequality is a characteristic-dependent linear rank inequality over fields whose characteristic does not divide* $t=\prod_i t_i$,

$$\mathrm{H}\left(C\right)\leq\frac{1}{m}\mathrm{H}\left(A_{e_j},B_{e_{S_i}},C:e_{S_i}\in\mathcal{B}',e_j\in\mathcal{B}'',C\in\mathcal{B}'''\right)+\mathrm{H}\left(C\mid A_{[e_n]}\right)$$

$$+\sum_{e_i\in[e_n]}\mathrm{I}\left(A_{[e_n]-e_i};C\right)+\sum_{e_{S_k}\in\mathcal{B}'}\left[\mathrm{H}\left(C\mid A_{e_i},B_{S_k}:i\notin S_k\right)+\mathrm{H}\left(B_{e_{S_k}}\mid A_{e_i}:i\in S_k\right)\right]$$

$$+\sum_{e_{S_k}\in\mathcal{B}'}\left[\nabla\left(A_{e_i}:i\notin S_k\right)+\nabla\left(A_{e_i}:i\in S_k\right)\right].$$

The first inequality does not in general hold over vector spaces whose characteristic does not divide t and the second inequality does not in general hold over vector spaces whose characteristic divides t. A counterexample would be in $V=\mathrm{GF}\left(p\right)^m$, take the vector spaces $A_{e_i}=\langle e_i\rangle$, $i\in[m]$, $B_{e_{S_j}}=\left\langle e_{S_j}\right\rangle$, $e_{S_j}\in\mathcal{B}'$, and $C=\langle\sum e_i\rangle$ Then, when p does not divide t, the first inequality does not hold; and when p divides t, the second inequality does not hold.

We prove the theorem.

Proof. By Lemmas 2.1.20 and 2.1.21, the subspaces $\bar{A}_{e_1},\ldots,\bar{A}_{e_n}$, $\bar{B}_{e_{S_{j_1}}},\ldots,\bar{B}_{e_{S_{j_{|\mathcal{B}'|}}}}$ and $\bar{C}$ satisfy hypothesis of the Proposition 2.1.18 in a finite field $\mathbb{F}$ whose characteristic divides t_k, we get

$$\mathrm{H}\left(\bar{B}_{e_{S_i}},\bar{A}_{e_j},\bar{C}:e_{S_i}\in\mathcal{B}',e_j\in\mathcal{B}'',\bar{C}\in\mathcal{B}'''\right)\leq m_k\mathrm{H}\left(\bar{C}\right). \tag{2.1.11}$$

On the other hand,

$$\mathrm{H}\left(\bar{C}\right)\leq\mathrm{I}\left(A_{[e_n]};C\right)\quad[\text{from }\bar{C}\leq C], \tag{2.1.12}$$

$$\mathrm{H}\left(\sum_{e_{S_k}\in\mathcal{B}'}B_{S_i}\mid\sum_{e_{S_k}\in\mathcal{B}'}\bar{B}_{S_1}\right)\leq\sum_{e_{S_k}\in\mathcal{B}'}\mathrm{H}\left(B_{e_{S_i}}\mid\bar{B}_{e_{S_i}}\right)\quad[\text{from Lemma 2.1.8}].$$

Therefore,

$$\mathrm{H}\left(\sum_{e_{S_k}\in\mathcal{B}'}B_{S_i}+\sum_{e_i\in\mathcal{B}''}A_{e_i}+C\mid\sum_{e_{S_k}\in\mathcal{B}'}\bar{B}_{S_i}+\sum_{e_i\in\mathcal{B}''}\bar{A}_{e_i}+\bar{C}\right)\leq\sum_{e_{S_k}\in\mathcal{B}'}\mathrm{H}\left(B_{e_{S_k}}\mid A_{e_i}:i\in S_k\right)$$

$$+\sum_{e_{S_k}\in\mathcal{B}'}\mathrm{H}\left(B_{e_{S_k}}\mid A_{e_i},C:i\notin S_k\right)+\left(|\mathcal{B}'|+1\right)\sum_{e_i\in\mathcal{B}''}\mathrm{H}\left(A_{e_i}\right)$$

$$+\left(|\mathcal{B}''|\,|\mathcal{B}'|+|\mathcal{B}''|+|\mathcal{B}'|+1\right)\nabla\left(C\right)-\left(|\mathcal{B}''|\,|\mathcal{B}'|+|\mathcal{B}''|\right)\mathrm{H}\left(C\right)$$

$$+\sum_{e_{S_k}\in\mathcal{B}'}\left[\nabla\left(A_{e_i}:i\in S_k,e_i\notin\mathcal{B}''\right)+\nabla\left(A_{e_i}:i\notin S_k,e_i\notin\mathcal{B}''\right)\right].$$

From (2.1.11) , (2.1.12), (2.1.5) and last inequality, we can obtain that the inequality in item (i) is true over fields whose characteristic divides t_k. We can do this for any $k=1,\ldots,s$. Noting that inequality (2.1.11) is also true for fields whose characteristic divides to t_s with $m_s<m_k$, we get that the inequality in item (i) is also true when $\prod_{i\leq k} t_i$.

To prove the inequality in item (ii), using Lemma 2.1.22, the vector subspaces A'_{e_1}, ..., A'_{e_n}, $\hat{B}_{e_{S_{j_1}}}$, ..., $\hat{B}_{e_{S_{j_{|\mathcal{B}'|}}}}$ and $\hat{C}$ satisfy hypothesis of Proposition 2.1.19 in a finite field $\mathbb{F}$ whose characteristic does not divide t, we get

$$m\mathrm{H}\left(\hat{C}\right)\leq\mathrm{H}\left(A'_{e_i},\hat{B}_{e_{S_j}},\hat{C}:e_{S_j}\in\mathcal{B}',e_i\in\mathcal{B}'',\hat{C}\in\mathcal{B}'''\right). \tag{2.1.13}$$

On the other hand,

$$\mathrm{H}\left(A'_{e_i},\hat{B}_{e_{S_j}},\hat{C}:e_{S_j}\in\mathcal{B}',e_i\in\mathcal{B}'',\hat{C}\in\mathcal{B}'''\right)\leq\mathrm{H}\left(A_{e_i},B_{e_{S_j}},C:e_{S_j}\in\mathcal{B}',e_i\in\mathcal{B}'',C\in\mathcal{B}'''\right). \tag{2.1.14}$$

From (2.1.13) , (2.1.10) and last inequality, we can derive the inequality (ii) over fields whose characteristic does not divide t. □

Corollary 2.1.24. *If the dimension of vector space V is at most $n-1$, then inequalities implicated in Theorem 2.1.23 are true over any field.*

Corollary 2.1.25. *If some vector space in Theorem 2.1.23 is the zero space, the inequalities implicated are linear rank inequalities.*

In case that the dimension of V is at most $n-1$, equation in Corollary 2.1.16 is trivial and therefore in the demonstration above there exists some $A'_{e_i}=O$ and $\hat{C}=\bar{C}=O$. This implies Corollary 2.1.24. The other corollary is also obtained in a similar way.

2.2 Two classes of inequalities

Below, it is shown a class of $\left\lfloor\frac{n-1}{2}\right\rfloor-2$ inequalities that are true over finite sets of primes (i.e. sets of the form $\{p:p\mid t\}$), and another class of $\left\lfloor\frac{n-1}{2}\right\rfloor-2$ inequalities that are true over co-finite sets of primes (i.e. sets of the form $\{p:p\nmid t\}$).

Example 2.2.1. Let $n\geq 7$ and t integer such that $2\leq t\leq\left\lfloor\frac{n-1}{2}\right\rfloor-1$ and $M(n,t)=n-t-2$. In Theorem 2.1.23, we take square matrices $B^t_{M(n,t)}$ as described in Figure 2.2.1 with column vectors of the form $B_i:=B_{e_{[M(n,t)]-i}}=c-e_i$, $A_i:=A_{e_i}=e_i$, with $c=\sum_{j\in[M(n,t)]}e_j$. The rank

$$\begin{array}{c} B_1 \cdots B_{t+1} A_{t+2} \cdots A_{M(n,t)} \\ \begin{pmatrix} 0 & \cdots & 1 & 0 & \cdots & 0 \\ 1 & \vdots & 1 & 0 & \vdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & 0 \\ 1 & \vdots & 1 & 0 & \vdots & 0 \\ 1 & \vdots & 0 & 0 & \vdots & \vdots \\ 1 & \vdots & 1 & 1 & \vdots & 0 \\ 1 & \vdots & \vdots & 0 & \vdots & 0 \\ 1 & \vdots & 1 & \vdots & \vdots & 0 \\ 1 & \cdots & 1 & 0 & \cdots & 1 \end{pmatrix} \end{array}$$

Figure 2.2.1: Matrix $B^t_{M(n,t)}$ whose rank is $M(n,t)$ or $M(n,t)-1$ according to the characteristic.

of $B^t_{M(n,t)}$ is $M(n,t)$ when $\mathrm{char}(\mathbb{F})$ does not divide t and is $M(n,t)-1$ in other case. We have $\left|\mathcal{B}'_{B^t_{M(n,t)}}\right| = t+1$, $\left|\mathcal{B}''_{B^t_{M(n,t)}}\right| = M(n,t)-t-1$, $\left|\mathcal{B}'''_{B^t_{M(n,t)}}\right| = 0$ and

$$\nabla(C) = \mathrm{H}\left(C \mid A_{[M(n,t)]}\right) + \sum_{i=1}^{M(n,t)} \mathrm{I}\left(A_{[M(n,t)]-i}; C\right)$$

$$\nabla(A_k) = \mathrm{I}\left(A_{[k-1]}; A_k\right),$$

$$\nabla(A_i : i \in [t+1]-k) = \mathrm{I}\left(A_{[k]}; A_{[k+1,t+1]}\right),$$

$$\nabla(A_i : i \in [M(n,t)]-k) = \mathrm{I}\left(A_{[k]}; A_{[k+1,M(n,t)]}\right), \text{ for each } k \in [t+1].$$

Then, for any A_1, A_2, ..., $A_{M(n,t)}$, B_1, B_2, ..., B_{t+1} and C subspaces of a finite dimensional vector space V over a finite field $\mathbb{F}$, we have:

(a) If $\mathrm{char}(\mathbb{F})$ divides t,

$$\mathrm{H}\left(B_{[t+1]}, A_{[t+2,M(n,t)]}\right) + (t+2)\left(M(n,t)-t-1\right)\mathrm{H}(C)$$

$$\leq \left(M(n,t)-1\right)\mathrm{I}\left(A_{[M(n,t)]}; C\right) + (t+2)\sum_{i=t+2}^{M(n,t)} \mathrm{H}(A_i)$$

$$+\left[(t+2)\left(M(n,t)-t\right)-1\right]\left(\mathrm{H}\left(C \mid A_{[M(n,t)]}\right) + \sum_{i=1}^{M(n,t)} \mathrm{I}\left(A_{[M(n,t)]-i}; C\right)\right)$$

$$+\sum_{i=1}^{t+1}\left(\mathrm{H}\left(B_i \mid A_i, C\right)+\mathrm{H}\left(B_i \mid A_{[M(n,t)]-i}\right)+\mathrm{I}\left(A_{[i]}; A_{[i+1,t+1]}\right)+\mathrm{I}\left(A_{[i-1]}; A_i\right)\right).$$

(b) If $\mathrm{char}\left(\mathbb{F}\right)$ does not divide t,

$$\mathrm{H}\left(C\right) \leq \frac{1}{M\left(n,t\right)}\mathrm{H}\left(B_{[t+1]}, A_{[t+2,M(n,t)]}\right)+\mathrm{H}\left(C \mid A_{[M(n,t)]}\right)+\sum_{i=1}^{M(n,t)}\mathrm{I}\left(A_{[M(n,t)]-i}; C\right)$$

$$+\sum_{i=1}^{t+1}\left(\mathrm{H}\left(C \mid A_i, B_i\right)+\mathrm{H}\left(B_i \mid A_{[M(n,t)]-i}\right)+\mathrm{I}\left(A_{[i]}; A_{[i+1,M(n,t)]}\right)+\mathrm{I}\left(A_{[i-1]}; A_i\right)\right).$$

Corollary 2.1.25 shows that each inequality presented in Example 2.2.1 cannot be deduced from a higher order inequality by nullifying some variables. In fact, using Corollary 2.1.24, we can say more about the class (a) of these inequalities: for $n \in \mathbb{N}$ and p prime, the function that counts all the powers of p less than or equal to n is denoted by $\varphi\left(n,p\right)$. In Example 2.2.1, for each power p^i less than or equal to $\left\lfloor\frac{n-1}{2}\right\rfloor-1$ is determined an inequality in n variables which is true over fields whose characteristic is p. Thus, $\varphi\left(\left\lfloor\frac{n-1}{2}\right\rfloor-1,p\right)$ inequalities in n variables, which are true over fields whose characteristic is p, are produced. By Corollary 2.1.24, each of these inequalities holds over any characteristic if the dimension of V is at most $n-p^i-3$. Hence, inequalities implied by the inequalities determined by p, ..., p^{i-1} are true over any vector space when the dimension is at most $n-p^{i-1}-3$ while the inequality determined by p^i does not hold over vector spaces of dimension $n-p^{i-1}-3$ and characteristics other than p. We have the next corollary.

Corollary 2.2.2. *For each $n \geq 7$ and p prime. There exist $\varphi\left(\left\lfloor\frac{n-1}{2}\right\rfloor-1,p\right)$ characteristic-dependent linear rank inequalities that are true over fields whose characteristic is p, such that the inequality determined by p^i is independent of all inequalities determined by p^j, $j<i$.*

3 Method II for Producing Inequalities

This method is developed with helping of the technique of the kernel presented in [23]. That technique was used for producing lower bounds on the information ratios in linear secret sharing from ports of Fano and non-Fano matroids over fields where these are not ideal. We note that this can be improved in order to produce characteristic-dependent linear rank inequalities that also imply lower bounds on the mentioned ratios. So, in this chapter as previous one, we show a theorem that produce inequalities. Initially, using a port of the Fano matroid as guide, we adapt some propositions of [23] in order to deduce a conditional characteristic-dependent linear rank inequality that we later turn into characteristic-dependent linear rank inequality; this is a particular case of the method. We then show the described theorem that produces inequalities using as guide non-singular matrices over some fields.

3.1 How to use access structures

We start by proving.

Lemma 3.1.1. *Let W, X_1, ..., X_m be vector subspaces of a finite dimensional vector space V over a finite field $\mathbb{F}$, such that*

- $W \leq \sum_i X_i$,
- $W \cap \left(\sum_{i \neq k} X_i \right) = O$ *for all* k.

Then, there exist subspaces $\bar{X}_i \leq X_i$, for $i = 1, \ldots, m$, such that

(i) $\bar{X}_k \cap \left(\sum_{i \neq k} X_i \right) = O$,

(ii) $\left(\bar{X}_1, \ldots, \bar{X}_m, W \right)$ *is a tuple of complementary vector subspaces,*

(iii) $\mathrm{H}(W) = \mathrm{H}(X_i')$.

Proof. In case $W = O$, we can take $\bar{X}_i = O$ for all i. Otherwise, we can assume

$$W, X_1, \ldots, X_m \neq O.$$

Let (e_i) be a basis of W. We remark that each e_i can be written as $\sum_j e_i^j$ with $e_i^j \in X_i$ by hypothesis. Define

$$\bar{X}_i = \left\langle e_i^j : j \right\rangle.$$

To prove item (i), we take $x \in \bar{X}_k \cap \left(\sum_{i \neq k} X_i \right)$. Then $x = \sum_j \alpha_j e_k^j$. So,

$$\sum_j \alpha_j e_j = \sum_i \alpha_i \sum_j e_i^j$$

$$= \sum_j \alpha_j e_k^j + \sum_{i \neq k} \alpha_i e_i^j.$$

Thus,

$$\sum_j \alpha_j e_j \in W \cap \left(\sum_{i \neq k} X_i \right),$$

which implies that $\sum_j \alpha_j e_j = O$ by hypothesis. Since (e_i) is a basis, $\alpha_i = 0$ for all i. In other words, $x = O$. Hence, (i) is true. In particular, this implies that $\bar{X}_k \cap \left(\sum_{i \neq k} \bar{X}_i \right) = O$, and since by definition $W \leq \sum_i \bar{X}_i$, it follows that (ii) is true. We also note $\bar{X}_i$ is generated by at most $\mathrm{H}(W)$-vectors; therefore, by Proposition 2.1.4 and (ii), we have (iii) is true. □

Lemma 3.1.2. *For any vector subspaces $X_1, \ldots, X_n$ of a finite dimensional vector space V over a finite field $\mathbb{F}$, we have*

$$\sum_i \mathrm{H}(X_i) - \mathrm{I}(X_1; \cdots; X_n) \leq \sum_{1<i} \mathrm{H}(X_1, X_i).$$

Proof. The proof is by induction. The case $n = 2$ gives a straightforward information identity. We suppose the case $n-1$ holds, and we show the case n,

$$\sum_i \mathrm{H}(X_i) - \mathrm{I}(X_1; \cdots; X_n) = \mathrm{H}(X_n) + \mathrm{H}(X_1 \cap \cdots \cap X_{n-1})$$

$$-\mathrm{I}(X_1 \cap \cdots \cap X_{n-1}; X_n) + \sum_{i \leq n-1} \mathrm{H}(X_i) - \mathrm{I}(X_1; \cdots; X_{n-1})$$

$$\leq \mathrm{H}(X_1 \cap \cdots \cap X_{n-1}, X_n) + \sum_{1<i \leq n-1} \mathrm{H}(X_1, X_i) \text{ [from cases } n = 2 \text{ and } n-1]$$

$$\leq \mathrm{H}(X_1, X_n) + \sum_{1<i \leq n-1} \mathrm{H}(X_1, X_i)$$

$$= \sum_{1<i} \mathrm{H}(X_1, X_i).$$

□

Remark 3.1.3. It can be used software such as Xitip to note that inequalities in previous lemma are in fact Shannon-information inequalities; nevertheless the vector space structure provides a simple proof in the class of linear random variables.

3.1.1 A particular case

We next define a characteristic-dependent linear rank inequalities using as guide a certain properties of the port of the Fano matroid at c: This port is given in Example 1.4.6. The following set is a subclass of authorized set:

$$\{a_1b_1, a_2b_2, a_3b_3, a_1a_2a_3\};$$

and the following set is a subclass of non-authorized set:

$$\{b_1a_2a_3, a_1b_2a_3, a_1a_2b_3, b_1b_2b_3\}.$$

The following lemmas abstract these properties:

Lemma 3.1.4. *Let A_1, A_2, A_3, B_1, B_2, B_3 and C be vector subspaces of a finite dimensional vector space V over a finite field $\mathbb{F}$, such that*

(i) *C is a subspace of each $A_{[3]}$, A_1+B_1, A_2+B_2, A_3+B_3.*

(ii) *$C\cap A_{[2,3]} = C\cap A_{1\cup 3} = C\cap A_{[2]} = O$,*

(iii) *$C\cap B_1 = C\cap B_2 = C\cap B_3 = O$.*

Then

$$4\mathrm{H}(C) \leq \mathrm{H}(A_1)+\mathrm{H}(A_2)+\mathrm{H}(A_3)+\mathrm{H}(\ker\phi), \tag{3.1.1}$$

where the linear mapping $\phi : C \to \frac{\bar{A}_1}{\bar{A}_1\cap\hat{A}_1}\oplus\frac{\bar{A}_2}{\bar{A}_2\cap\hat{A}_2}\oplus\frac{\bar{A}_3}{\bar{A}_3\cap\hat{A}_3}$ is given by

$$\phi(c) := \phi(a_1+a_2+a_3) = [a_1]_{\bar{A}_1\cap\hat{A}_1} + [a_2]_{\bar{A}'_2\cap\hat{A}_2} + [a_3]_{\bar{A}_3\cap\hat{A}_3},$$

when we take $\bar{X}_i = \bar{A}_i$ with $m=3$ and $X_i = A_i$ in Lemma 3.1.1; and we take $\bar{X}_1 = \hat{A}_i$ with $m=2$, $X_1 = A_i$ and $X_2 = B_i$ in Lemma 3.1.1, for each i.

Proof. We remark that in case $C = O$, the inequality is trivial and therefore $\phi = 0$. When some A_i or B_i is null, it is easy to prove that $C = O$. We thus assume that all subspaces are

not null. So, we have the inequality

$$\mathrm{H}\left(\frac{C}{\ker\phi}\right) \leq \mathrm{H}\left(\frac{\bar{A}_1}{\bar{A}_1 \cap \hat{A}_1}\right) + \mathrm{H}\left(\frac{\bar{A}_2}{\bar{A}_2 \cap \hat{A}_2}\right) + \mathrm{H}\left(\frac{\bar{A}_3}{\bar{A}_3 \cap \hat{A}_3}\right).$$

Then,

$$\mathrm{H}(C) - \mathrm{H}(\ker\phi) \leq \mathrm{H}\left(\bar{A}_1\right) + \mathrm{H}\left(\bar{A}_2\right) + \mathrm{H}\left(\bar{A}_3\right)$$
$$-\mathrm{I}\left(\bar{A}_1; \hat{A}_1\right) - \mathrm{I}\left(\bar{A}_2; \hat{A}_2\right) - \mathrm{I}\left(\bar{A}_3; \hat{A}_3\right).$$

Therefore,

$$4\mathrm{H}(C) - \mathrm{H}(\ker\phi) \leq \mathrm{H}\left(\bar{A}_1\right) + \mathrm{H}\left(\hat{A}_1\right) - \mathrm{I}\left(\bar{A}_1; \hat{A}_1\right)$$
$$+\mathrm{H}\left(\bar{A}_2\right) + \mathrm{H}\left(\hat{A}_2\right) - \mathrm{I}\left(\bar{A}_2; \hat{A}_2\right) + \mathrm{H}\left(\bar{A}_3\right) + \mathrm{H}\left(\hat{A}_3\right) - \mathrm{I}\left(\bar{A}_3; \hat{A}_3\right)$$
[from (iii) in Lemma 3.1.1]
$$4\mathrm{H}(C) - \mathrm{H}(\ker\phi) \leq \mathrm{H}\left(\bar{A}_1, \hat{A}_1\right) + \mathrm{H}\left(\bar{A}_2, \hat{A}_2\right) + \mathrm{H}\left(\bar{A}_3, \hat{A}_3\right)$$
[straightforward information equality].

Noting that $\mathrm{H}\left(\bar{A}_i, \hat{A}_i\right) \leq \mathrm{H}(A_i)$, we get the desired inequality. □

Now, we produce a conditional characteristic-dependent linear rank inequality.

Lemma 3.1.5. *Let A_1, A_2, A_3, B_1, B_2, B_3 and C be vector subspaces of a finite dimensional vector space V over a finite field $\mathbb{F}$ with characteristic other than two, such that*

(i) *C is a subspace of each $A_{[3]}$, $A_1 + B_1$, $A_2 + B_2$ and $A_3 + B_3$.*

(ii) *$C \cap \left(A_{[2,3]} + B_1\right) = C \cap (A_{1\cup 3} + B_2) = C \cap \left(A_{[2]} + B_3\right) = O$.*

(iii) *$C \cap B_{[3]} = O$.*

Then,

$$4\mathrm{H}(C) \leq \mathrm{H}(A_1) + \mathrm{H}(A_2) + \mathrm{H}(A_3).$$

Proof. From (ii), we can derive

$$C \cap A_{[2,3]} = C \cap A_{1\cup 3} = C \cap A_{[2]} = O$$

and

$$C \cap B_1 = C \cap B_2 = C \cap B_3 = O.$$

From this and (i), Lemma 3.1.1 can be applied. Hence, the inequality 3.1.1 is true, and it is enough to show that $\ker(\phi) = O$. We take $c = a_1 + a_2 + a_3 \in C$ such that $\phi(c) = O$, where

$a_i \in \bar{A}_i$ and we check that $c = O$. By definition, $a_i \in \bar{A}_i \cap \hat{A}_i$. From (i) in Lemma 3.1.1, there exists $b_i \in \hat{B}_i$ for each $i = 1, 2, 3$ such that $a_i + b_i \in C$. Hence,

$$a_2 + a_3 - b_1 = c - (a_1 + b_1) \in C \cap \left(A_{[2,3]} + B_1\right),$$

$$a_1 + a_3 - b_2 = c - (a_2 + b_2) \in C \cap \left(A_{1\cup 3} + B_2\right),$$

$$a_1 + a_2 - b_3 = c - (a_3 + b_3) \in C \cap \left(A_{[2]} + B_3\right),$$

but from (ii),

$$a_2 + a_3 = b_1,$$

$$a_1 + a_3 = b_2,$$

$$a_1 + a_2 = b_3.$$

Then,

$$b_1 + b_2 + b_3 = (a_2 + a_3) + (a_1 + a_3) + (a_1 + a_2) = 2c.$$

From (iii), $2c = O$. As the characteristic of $\mathbb{F}$ is other than two, it follows $c = O$. □

We produce a characteristic-dependent linear rank inequality that is true over fields whose characteristic is other than two.

Theorem 3.1.6. *Let A_1, A_2, A_3, B_1, B_2, B_3 and C be vector subspaces of a finite dimensional vector space V over a finite field $\mathbb{F}$. The following inequality is a characteristic-dependent linear rank inequality over fields with characteristic other than 2:*

$$\mathrm{H}(C) \leq \frac{1}{4}\left(\mathrm{H}(A_1) + \mathrm{H}(A_2) + \mathrm{H}(A_3)\right) + \mathrm{H}(C \mid A_1, A_2, A_3)$$

$$+\mathrm{I}(C; B_1, B_2, B_3) + \mathrm{H}(C \mid A_1, B_1) + \mathrm{H}(C \mid A_2, B_2) + \mathrm{H}(C \mid A_3, B_3)$$

$$+\mathrm{I}(C; A_2, A_3, B_1) + \mathrm{I}(C; A_1, A_3, B_2) + \mathrm{I}(C; A_1, A_2, B_3).$$

Proof. Let

$$C^{(0)} := C \cap A_{[3]} \cap (A_1 + B_1) \cap (A_2 + B_2) \cap (A_3 + B_3);$$

we have

$$\mathrm{H}\left(C \mid C^{(0)}\right) \leq \mathrm{H}\left(C \mid A_{[3]}\right) + \mathrm{H}(C \mid A_1, B_1) + \mathrm{H}(C \mid A_2, B_2) + \mathrm{H}(C \mid A_3, B_3).$$

Recursively, define $C^{(1)}$, a subspace of $C^{(0)}$ which is a complementary subspace to $A_{[2,3]} + B_1$ in

$$C^{(0)} + \left(A_{[2,3]} + B_1\right),$$

we also have

$$\begin{aligned}\mathrm{H}\left(C^{(0)} \mid C^{(1)}\right) &= \mathrm{I}\left(C^{(0)}; A_{[2,3]}, B_1\right) \\ &\leq \mathrm{I}\left(C; A_{[2,3]}, B_1\right);\end{aligned}$$

define $C^{(2)}$, a subspace of $C^{(1)}$ which is a complementary subspace to $A_{1\cup 3} + B_2$ in

$$C^{(1)} + \left(A_{1\cup 3} + B_2\right);$$

we also have

$$\begin{aligned}\mathrm{H}\left(C^{(1)} \mid C^{(2)}\right) &= \mathrm{I}\left(C^{(1)}; A_{1\cup 3}, B_2\right) \\ &\leq \mathrm{I}\left(C; A_{1\cup 3}, B_2\right);\end{aligned}$$

and define $C^{(3)}$, a subspace of $C^{(2)}$ which is a complementary subspace to $A_{[2]} + B_3$ in

$$C^{(2)} + \left(A_{[2]} + B_3\right);$$

we also have

$$\begin{aligned}\mathrm{H}\left(C^{(2)} \mid C^{(3)}\right) &= \mathrm{I}\left(C^{(2)}; A_{[2]}, B_3\right) \\ &\leq \mathrm{I}\left(C; A_{[2]}, B_3\right);\end{aligned}$$

Now define by $\hat{C}$, a subspace of $C^{(3)}$ which is a complementary subspace to $B_{[3]}$ in $C^{(3)} + B_{[3]}$; we also have

$$\begin{aligned}\mathrm{H}\left(C^{(3)} \mid \hat{C}\right) &= \mathrm{I}\left(C^{(3)}; B_{[3]}\right) \\ &\leq \mathrm{I}\left(C; B_{[3]}\right).\end{aligned}$$

Using all these inequalities we can derive

$$\begin{aligned}\mathrm{H}\left(C \mid \hat{C}\right) &= \mathrm{H}\left(C \mid C^{(0)}\right) + \mathrm{H}\left(C^{(0)} \mid C^{(1)}\right) + \mathrm{H}\left(C^{(1)} \mid C^{(2)}\right) \\ &\quad + \mathrm{H}\left(C^{(2)} \mid C^{(3)}\right) + \mathrm{H}\left(C^{(3)} \mid \hat{C}\right) \\ &\qquad\qquad [\text{definition of } \hat{C}] \\ &\leq \mathrm{H}\left(C \mid A_{[3]}\right) + \mathrm{H}\left(C \mid A_1, B_1\right) + \mathrm{H}\left(C \mid A_2, B_2\right) + \mathrm{H}\left(C \mid A_3, B_3\right) \\ &\quad + \mathrm{I}\left(C; A_{[2,3]}, B_1\right) + \mathrm{I}\left(C; A_{1\cup 3}, B_2\right) + \mathrm{I}\left(C; A_{[2]}, B_3\right) + \mathrm{I}\left(C; B_{[3]}\right).\end{aligned}$$

By definition of $\hat{C}$, we also have that A_1, A_2, A_3, B_1, B_2, B_3 and $\hat{C}$ satisfy Lemma 3.1.5.

Hence

$$4\mathrm{H}\left(\hat{C}\right) \leq \mathrm{H}\left(A_1\right) + \mathrm{H}\left(A_2\right) + \mathrm{H}\left(A_3\right).$$

From this and previous inequality, we obtain the desired characteristic-dependent linear rank inequality. □

We remark that inequality does not in general hold over fields with characteristic two, and of course taking the columns of a representation matrix of the Fano matroid, we can check it.

3.1.2 Other access structures

For a $m \times m$ binary matrix $B = (B^i) = (e_{S_i})$, with $S_i = \left\{j : B_{(j,i)} = 1\right\}$, we again use the sets:

$$\mathcal{B}' := \left\{e_{S_i} : 1 < |S_i| < m\right\},$$

$$\mathcal{B}'' := \left\{e_{S_i} : |S_i| = 1\right\},$$

and in this charter we always take

$$\mathcal{B}''' := \left\{e_{S_i} : |S_i| = m\right\} = \emptyset.$$

We suppose that $|\det(B)| = t > 1$, for some $t \in \mathbb{N}$.

This type of matrices can be used to define matroid ports which are ideal over some fields (representable matroids). We consider an access structure on

$$P := \left\{b_{e_{S_j}} : e_{S_j} \in \mathcal{B}'\right\} \cup \left\{a_{e_i} : i \in [m]\right\},$$

such that the following set is a subclass of the collection of minimal authorized sets:

$$\left\{\left(a_{e_i}\right)_{i \notin S_j} b_{e_{S_j}} : e_{S_j} \in \mathcal{B}'\right\} \cup \left\{a_{e_1} \cdots a_{e_m}\right\}$$

and the following set is a subclass of the class of non-authorized sets:

$$\left\{\left(a_{e_i}\right)_{i \in S_j} b_{e_{S_j}} : e_{S_j} \in \mathcal{B}'\right\}.$$

Let P_B be the subset of participants indexed by the columns of B. When we can add P_B to the subclass of minimal authorized sets or the subclass of non-authorized sets; we produce at least two different classes of access structures. In the following sections, each participant is associated to a vector spaces: a_{e_i} is associated to a vector subspace A_{e_i}; b_{e_i} is associated to a

vector subspace B_{e_i}; the dealer $p = c$ is associated to a vector subspace C. Then, the classes defined above are used as a guide to determine the properties that must be satisfied by the vector spaces in order to derive some inequalities. The following proposition is obtained using Lemma 3.1.1. We note that it expresses the fact that $a_{e_1} \cdots a_{e_m}$, $(a_{e_i})_{i \notin S_j}\, b_{e_{S_j}}$ are minimal authorized sets.

Proposition 3.1.7. *Let A_{e_i}, for $i \in [m]$, $B_{e_{S_i}}$, for $e_{S_j} \in \mathcal{B}'$, and C be vector subspaces of a finite dimensional vector space V such that*

- $C \leq A_{[e_m]} \cap \left(\sum_{i \notin S_j} A_{e_i} + B_{e_{S_j}} \right)$ *, for each j,*
- $C \cap A_{[e_m]-e_j} = C \cap \left(\sum_{j \notin S_i, j \neq k} A_{e_j} + B_{e_{S_i}} \right) = O$*, for all j, $e_{S_i} \in \mathcal{B}'$ and $k \notin S_i$.*

Then, we have vector subspaces $\bar{A}_{e_i} \leq A_{e_i}$, $i \in [m]$; $A_{e_i}^{S_j} \leq A_{e_i}$ for each $i \notin S_j$ and $\hat{B}_{e_{S_i}} \leq B_{e_{S_i}}$ for each $e_{S_i} \in \mathcal{B}'$ such that

- $\left(\bar{A}_{e_1}, \cdots, \bar{A}_{e_m}, C\right)$ *is a tuple of complementary vector subspaces,*
- $\left(A_{e_i}^{S_j}, \hat{B}_{e_{S_j}}, C : i \notin S_j\right)$*, for each $e_{S_j} \in \mathcal{B}'$, is a tuple of complementary vector subspaces,*
- *the dimension of any of these subspaces is* $\mathrm{H}(C)$*,*
- *these subspaces are unique except isomorphism.*

3.1.2.1 A convenient linear mapping

We can ensure that the following mapping is well-defined by Proposition 3.1.7.

Definition 3.1.8. We define the following linear mapping

$$\begin{array}{c} \varphi_B : C \to \bigoplus_i \frac{\bar{A}_{e_i}}{(\bigcap \mathcal{A}_{e_i}) \cap \bar{A}_{e_i}} \\ c \longmapsto \varphi_B(c) := \varphi_B\left(\sum_i a_i\right) = \sum_i [a_i]_{(\bigcap \mathcal{A}_{e_i}) \cap \bar{A}_{e_i}} \end{array},$$

where

$$\mathcal{A}_{e_i} := \left\{ A_{e_i}^{S_j} : i \notin S_j \text{ for some } j \right\};$$

we take $\mathcal{A}_{e_i}$ as $\{O\}$, in case that $i \in S_j$ for all j.

Remark 3.1.9. There is a correspondence between $\mathcal{A}_{e_i}$ and the subset of columns of B given by

$$\mathcal{B}_{e_i} := \left\{ e_{S_j} : i \notin S_j \right\};$$

again, we take $\mathcal{B}_{e_i}$ as $\{O\}$, in case that $i \in S_j$ for all j.

Lemma 3.1.10. *For any vector subspaces $A_{e_1}, \ldots, A_{e_m}$, $B_{e_{S_{j_1}}}, \ldots, B_{e_{S_{j_{|\mathcal{B}'|}}}}$ and C of a finite dimensional vector space V over a finite field $\mathbb{F}$ such that*

(i) $C \leq A_{[e_m]} \cap \left(\sum_{j \notin S_i} A_{e_j} + B_{e_{S_i}} \right)$, *for each* $e_{S_i} \in \mathcal{B}'$.

(ii) $C \cap A_{[e_m]-e_i} = O$, *for each* i.

(iii) $C \cap \left(\sum_{j \notin S_i, j \neq k} A_{e_j} + B_{e_{S_i}} \right) = O$, *for all* $e_{S_i} \in \mathcal{B}'$ *and* $k \notin S_i$.

Then,

$$\left[1 + \sum_i |\mathcal{B}_{e_i}| \right] \mathrm{H}(C) \leq \sum_i |\mathcal{B}_{e_i}| \, \mathrm{H}(A_{e_i}) + \mathrm{H}(\ker(\varphi_B)) .$$

Proof. By definition of φ, we can derive the inequality

$$\mathrm{H}\left(\frac{C}{\ker(\varphi_B)} \right) \leq \sum_i \mathrm{H}\left(\frac{\bar{A}_{e_i}}{(\bigcap \mathcal{A}_{e_i}) \cap \bar{A}_{e_i}} \right).$$

So

$$\mathrm{H}(C) - \mathrm{H}(\ker(\varphi_B)) \leq \sum_i \left[\mathrm{H}\left(\bar{A}_{e_i} \right) - \mathrm{I}\left(\bar{A}_{e_i}; \bigcap \mathcal{A}_{e_i} \right) \right]$$

then

$$\mathrm{H}(C) - \mathrm{H}(\ker\varphi_B) + \sum_i \sum_{e_{S_j} \in \mathcal{B}_{e_i}} \mathrm{H}\left(A_{e_i}^{S_j} \right) \leq \sum_i \left[\mathrm{H}\left(\bar{A}_{e_i} \right) + \sum_{e_{S_j} \in \mathcal{B}_{e_i}} \mathrm{H}\left(A_{e_i}^{S_j} \right) - \mathrm{I}\left(\bar{A}_{e_i}; \bigcap \mathcal{A}_{e_i} \right) \right],$$

$$\leq \sum_i \sum_{e_{S_j} \in \mathcal{B}_{e_i}} \mathrm{H}\left(\bar{A}_{e_i}, A_{e_i}^{S_j} \right), \text{ [from Lemma 3.1.2].}$$

Since $\mathrm{H}\left(A_{e_i}^{S_j} \right) = \mathrm{H}(C)$, $\sum_{e_{S_j} \in \mathcal{B}_{e_i}} 1 = |\mathcal{B}_{e_i}|$ and $\bar{A}_{e_i}, A_{e_i}^{S_j} \leq A_{e_i}$, we get

$$\mathrm{H}(C) - \mathrm{H}(\ker(\varphi_B)) + \sum_i |\mathcal{B}_{e_i}| \, \mathrm{H}(C) \leq \sum_i |\mathcal{B}_{e_i}| \, \mathrm{H}(A_{e_i}) ,$$

which implies the desired inequality. □

Lemma 3.1.11. *For any vector subspaces* $A_{e_1}, \ldots, A_{e_m}$, $B_{e_{S_{j_1}}}, \ldots, B_{e_{S_{j_{|\mathcal{B}'|}}}}$ *and* C *of a finite dimensional vector space* V *over a finite field* $\mathbb{F}$ *whose characteristic does not divide* t*, such that*

(i) $C \leq A_{[e_m]} \cap \left(\sum_{j \notin S_i} A_{e_j} + B_{e_{S_i}} \right)$, *for each* $e_{S_i} \in \mathcal{B}'$.

(ii) $C \cap A_{[e_m]-e_j} = C \cap \left(\sum_{j \in S_i} A_{e_j} + B_{e_{S_i}} \right) = C \cap \left(\sum_{j \notin S_i, j \neq k} A_{e_j} + B_{e_{S_i}} \right) = O$, *for all* $e_{S_i} \in \mathcal{B}'$ *and* $k \notin S_i$.

(iii) *$C \cap \mathcal{B} = O$, where $\mathcal{B}$ is the sum of all vector subspaces indexed by the columns of B.*

Then

$$\ker(\varphi_B) = O.$$

Proof. We take $c = \sum_i a_i \in C$ such that $\varphi_B(c) = O$, where $a_i \in \bar{A}_i$, and we have to show $c = O$. By definition of φ_B,

$$a_i \in \bar{A}_{e_i} \cap \left(\bigcap_{e_{S_j} \in \mathcal{B}_{e_i}} A_{e_i}^{S_j} \right).$$

Hence, $a_i \in A_{e_i}^{S_j}$ for all $e_{S_j} \in \mathcal{B}_{e_i}$, and therefore

$$\sum_{j \notin S_i} a_j \in \sum_{j \notin S_i} A_{e_j}^{S_i}.$$

From (i) in Lemma 3.1.1, there exists $b_i \in \hat{B}_{e_{S_i}}$ for each $e_{S_i} \in \mathcal{B}'$ such that $\sum_{j \notin S_i} a_j + b_i \in C$. Hence,

$$\sum_{j \in S_i} a_j - b_i = \sum_i a_i - \left(\sum_{j \notin S_i} a_j + b_i \right) \in C \cap \left(\sum_{j \in S_i} A_{e_j} + B_{e_{S_i}} \right),$$

but from (ii), this implies

$$\sum_{j \in S_i} a_j = b_i \text{ for all } e_{S_i} \in \mathcal{B}'.$$

These equations define the following matrix equation

$$B^T \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_{|\mathcal{B}'|} \\ b^1 \\ \vdots \\ b^{|\mathcal{B}''|} \end{pmatrix}, \tag{3.1.2}$$

where the vectors $b^1, \ldots, b^{|\mathcal{B}''|}$ are omitted when $\mathcal{B}''$ is empty; in other case, b^i is set to be a_i if $e_i \in \mathcal{B}''$. Since $\operatorname{char}(\mathbb{F})$ does not divide $t = |\det(B)|$, the matrix B^T is non-singular. Therefore, each a_i can be written as a linear combination of b_1, …, $b_{|\mathcal{B}'|}$, b^1, …, $b^{|\mathcal{B}''|}$, which implies that $c \in B$. From (iii), it follows $c = O$. □

Corollary 3.1.12. *For any vector subspaces $A_{e_1}, \ldots, A_{e_m}$, $B_{e_{S_{j_1}}}, \ldots, B_{e_{S_{j_{|\mathcal{B}'|}}}}$ and C of a finite dimensional vector space V over a finite field $\mathbb{F}$, such that*

(i) $C \leq A_{[e_m]} \cap \left(\sum_{j \notin S_i} A_{e_j} + B_{e_{S_i}} \right)$, *for each* $e_{S_i} \in \mathcal{B}'$.

(ii) $C \cap A_{[e_m]-e_j} = C \cap \left(\sum_{j \in S_i} A_{e_j} + B_{e_{S_i}} \right) = C \cap \left(\sum_{j \notin S_i, j \neq k} A_{e_j} + B_{e_{S_i}} \right) = O$, *for all* $e_{S_i} \in \mathcal{B}'$ *and* $k \notin S_i$.

Then, the mapping

$$\begin{aligned} \phi_B^k : \ker(\varphi_B) &\to B_{e_{S_k}} \\ c \longmapsto \phi_B^k(c) &:= \sum_{j \in S_k} a_j = b_k \end{aligned}$$

is an one-to-one well-defined linear function for each $e_{S_k} \in \mathcal{B}'$. *Also, if the* k*-column of* B *is a linear combination of the columns of the submatrix of* B *denoted by* B_X, $k \notin X$. *Then,*

$$\phi_B^k(\ker(\varphi_B)) \subseteq \sum_{e_i \in B_X \cap \mathcal{B}''} A_{e_i} + \sum_{e_{S_i} \in B_X \cap \mathcal{B}'} B_{e_{S_i}}.$$

Proof. We can follow line-by-line the proof of the previous lemma to obtain that there exists an unique $b_k \in \left(\sum_{j \in S_k} \bar{A}_j \right) \cap \hat{B}_{e_{S_k}} \subseteq B_{e_{S_k}}$. So ϕ_B^k is well-defined. Since the written of each $c \in \ker(\varphi_B)$ is unique, ϕ_B^k is also an one-to-one linear mapping. Also, if the k-column of B is a linear combination of the columns of B_X, from equation (3.1.2), we have that b_k is a linear combination of $(b_j)_{j \in B_X} \cup (b^j)_{j \in B_X}$. Therefore, $b_k \in \sum_{e_i \in B_X \cap \mathcal{B}''} A_{e_i} + \sum_{e_{S_i} \in B_X \cap \mathcal{B}'} B_{e_{S_i}}$. □

3.1.2.2 Characteristic-dependent linear rank inequalities

Theorem 3.1.13. *For a* $m \times m$ *binary matrix* B *such that* $\mathcal{B}''' = \emptyset$ *and* $|\det(B)| = t \in \mathbb{N}$, $t > 1$. *Let* $A_{e_1}, \ldots, A_{e_m}$, $B_{e_{S_{j_1}}}, \ldots, B_{e_{S_{j_{|\mathcal{B}'|}}}}$ *and* C *be vector subspaces of a finite dimensional vector space* V *over* $\mathbb{F}$. *We have*

- *The following inequality is a characteristic-dependent linear rank inequality over fields whose characteristic does not divide* t*:*

$$\begin{aligned} \mathrm{H}(C) \leq \frac{1}{1 + \sum_i |\mathcal{B}_{e_i}|} \sum_i |\mathcal{B}_{e_i}| \, \mathrm{H}(A_{e_i}) + \mathrm{H}\left(C \mid A_{[e_m]}\right) + \mathrm{I}\left(C; A_{e_i}, B_{e_{S_j}} : e_i \in \mathcal{B}'', e_{S_j} \in \mathcal{B}'\right) \\ + \sum_i \mathrm{I}\left(C; A_{[e_m]-e_i}\right) + \sum_{e_{S_h} \in \mathcal{B}', i \notin S_h.} \mathrm{I}\left(C; A_{e_j}, B_{e_{S_h}} : j \notin S_h, j \neq i\right) \\ + \sum_{e_{S_i} \in \mathcal{B}'} \left[\mathrm{H}\left(C \mid A_{e_j}, B_{e_{S_i}}, j \notin S_i\right) + \mathrm{I}\left(C; A_{e_j}, B_{e_{S_i}} : j \in S_i\right) \right]. \end{aligned}$$

- *Fixed $k \in [m]$ such that $e_{S_k} \in \mathcal{B}'$. The following inequality is a characteristic-dependent linear rank inequality over fields whose characteristic divides t:*

$$\mathrm{H}(C) \leq \frac{1}{2+\sum_i |\mathcal{B}_{e_i}|}\left[\sum_i |\mathcal{B}_{e_i}|\,\mathrm{H}(A_{e_i}) + \mathrm{H}\left(B_{e_{S_k}}\right)\right] + \mathrm{H}\left(C \mid A_{e_i}, B_{e_{S_j}} : e_i \in \mathcal{B}'', e_{S_j} \in \mathcal{B}'\right)$$

$$+\mathrm{H}\left(C \mid A_{[e_m]}\right) + \sum_{e_{S_i} \in \mathcal{B}'} \mathrm{H}\left(C \mid A_{e_j}, B_{e_{S_i}} : j \notin S_i\right)$$

$$+\sum_i \mathrm{I}\left(C; A_{[e_m]-e_i}\right) + \sum_{e_{S_h} \in \mathcal{B}', i \notin S_h.} \mathrm{I}\left(C; A_{e_j}, B_{e_{S_h}} : j \notin S_h, j \neq i\right)$$

$$+ \sum_{e_{S_i} \in \mathcal{B}'} \mathrm{I}\left(C; A_{e_j}, B_{e_{S_i}} : j \in S_i\right) + \sum_i \mathrm{I}\left(C; A_{e_j}, B_{e_{S_i}} : e_{S_j} \in \mathcal{B}', e_j \in \mathcal{B}'', j \neq i\right).$$

The inequalities do not in general hold over fields whose characteristic is different to the mentioned. As in Theorem 2.1.12, a counterexample would be in $V = \mathrm{GF}(p)^m$, take the vector spaces $A_{e_i} = \langle e_i \rangle$, $e_i \in [e_m]$, $B_{e_{S_j}} = \left\langle e_{S_j} \right\rangle$, $e_{S_j} \in \mathcal{B}'$, and $C = \langle \sum e_i \rangle$ Then, when p divides t, the first inequality does not hold; and when p does not divide t, the second inequality does not hold.

Proof. To prove the first inequality: let $\mathbb{F}$ be a finite field whose characteristic does not divide t. Let

$$C^{\langle 0 \rangle} := C \cap A_{[e_m]} \cap \left[\bigcap_{e_{S_i} \in \mathcal{B}'} \left(\sum_{j \notin S_i} A_{e_j} + B_{e_{S_i}}\right)\right].$$

We have

$$\mathrm{H}\left(C \mid C^{\langle 0 \rangle}\right) \leq \mathrm{H}\left(C \mid A_{[e_m]}\right) + \sum_{e_{S_i} \in \mathcal{B}'} \mathrm{H}\left(C \mid A_{e_j}, B_{e_{S_i}} : j \notin S_i\right).$$

Recursively, for $i \in [m]$, denote by $C^{\langle i \rangle}$, a subspace of $C^{\langle i-1 \rangle}$ which is a complementary subspace to $\sum_{j \neq i} A_{e_j}$ in

$$C^{\langle i-1 \rangle} + \sum_{j \neq i} A_{e_j}.$$

We have

$$\mathrm{H}\left(C^{\langle i-1 \rangle} \mid C^{\langle i \rangle}\right) \leq \mathrm{I}\left(C; A_{e_j} : j \neq i\right).$$

Let $C^{[0]}_{e_{S_{j_1}}} = C^{\langle m \rangle}$ and recursively, for each $i \notin S_{j_1}.$, denote by $C^{[i]}_{e_{S_{j_1}}}$, a subspace of $C^{[i-1]}_{e_{S_{j_1}}}$ which is a complementary subspace to $\sum_{j \notin S_{j_1}, j \neq i} A_{e_j} + B_{e_{S_{j_1}}}$ in

$$C^{[i-1]}_{e_{S_{j_1}}} + \sum_{j \notin S_{j_1}, j \neq i} A_{e_j} + B_{e_{S_{j_1}}}.$$

We have

$$\mathrm{H}\left(C_{e_{S_{j_1}}}^{[i-1]} \mid C_{e_{S_{j_1}}}^{[i]}\right) \leq \mathrm{I}\left(C; A_{e_j}, B_{e_{S_{j_1}}} : j \notin S_{j_1}, j \neq i\right).$$

In a similar way, we define $C_{e_{S_{j_2}}}^{[0]} = C_{e_{S_{j_1}}}^{[m]}$, ..., $C_{e_{S_{j_{|\mathcal{B}'|}}}}^{[0]} = C_{e_{S_{j_{|\mathcal{B}'|-1}}}}^{[m]}$ until to find a subspace $C^{(0)} := C_{e_{S_{j_{|\mathcal{B}'|}}}}^{[m]}$ that holds

$$\mathrm{H}\left(C^{\langle m\rangle} \mid C^{(0)}\right) \leq \sum_{e_{S_h} \in \mathcal{B}', i \notin S_h.} \mathrm{I}\left(C; A_{e_j}, B_{e_{S_h}} : j \notin S_h, j \neq i\right).$$

Recursively, for i, with $e_{S_i} \in \mathcal{B}'$, denote by $C^{(i)}$, a subspace of $C^{(i-1)}$ which is a complementary subspace to $\sum_{j \in S_i} A_{e_j} + B_{e_{S_i}}$ in

$$C^{(i-1)} + \left(\sum_{j \in S_i} A_{e_j} + B_{e_{S_i}}\right).$$

We also have

$$\mathrm{H}\left(C^{(i-1)} \mid C^{(i)}\right) \leq \mathrm{I}\left(C^{(i-1)}; A_{e_j}, B_{e_{S_i}} : j \in S_i\right).$$

Define by $\hat{C}$, a subspace of $C^{(|\mathcal{B}'|)}$ which is a complementary subspace to

$$\mathcal{B} = \left(\sum_{e_{S_i} \in \mathcal{B}'} B_{e_{S_i}}\right) + \left(\sum_{e_i \in \mathcal{B}''} A_{e_i}\right)$$

in

$$C^{(|\mathcal{B}'|)} + \mathcal{B}.$$

We have

$$\mathrm{H}\left(C^{(|\mathcal{B}'|)} \mid \hat{C}\right) \leq \mathrm{I}\left(C; A_{e_i}, B_{e_{S_j}} : e_i \in \mathcal{B}'', e_{S_j} \in \mathcal{B}'\right).$$

Hence,

$$\begin{aligned}
\mathrm{H}\left(C \mid \hat{C}\right) &= \mathrm{H}\left(C \mid C^{\langle 0\rangle}\right) + \mathrm{H}\left(C^{\langle 0\rangle} \mid C^{\langle m\rangle}\right) + \mathrm{H}\left(C^{\langle m\rangle} \mid C^{(0)}\right) \\
&\quad + \mathrm{H}\left(C^{(0)} \mid C^{(|\mathcal{B}'|)}\right) + \mathrm{H}\left(C^{(|\mathcal{B}'|)} \mid \hat{C}\right) \\
&\leq \mathrm{H}\left(C \mid A_{[e_m]}\right) + \sum_{e_{S_i} \in \mathcal{B}'} \mathrm{H}\left(C \mid A_{e_j}, B_{e_{S_i}} : j \notin S_i\right) \\
&\quad + \sum_i \mathrm{I}\left(C; A_{[e_m]-e_i}\right) + \sum_{e_{S_h} \in \mathcal{B}', i \notin S_h.} \mathrm{I}\left(C; A_{e_j}, B_{e_{S_h}} : j \notin S_h, j \neq i\right) \\
&\quad + \sum_{e_{S_i} \in \mathcal{B}'} \mathrm{I}\left(C; A_{e_j}, B_{e_{S_i}} : j \in S_i\right) + \mathrm{I}\left(C; A_{e_i}, B_{e_{S_j}} : e_i \in \mathcal{B}'', e_{S_j} \in \mathcal{B}'\right).
\end{aligned}$$

Since $A_{e_1}, \ldots, A_{e_m},\ B_{e_{S_{j_1}}}, \ldots, B_{e_{S_{j_{|\mathcal{B}'|}}}}$ and $\hat{C}$ satisfy hypothesis in Lemma 3.1.11, we have $\ker(\varphi_B) = O$. Therefore, as these spaces also satisfy hypothesis in Lemma 3.1.10, it follows

$$\left[1 + \sum_i |\mathcal{B}_{e_i}|\right] \mathrm{H}\left(\hat{C}\right) \leq \sum_i |\mathcal{B}_{e_i}| \, \mathrm{H}\left(A_{e_i}\right).$$

Using the last two inequalities, we can obtain the described inequality:

$$\mathrm{H}(C) - \mathrm{H}\left(C \mid A_{[e_m]}\right) - \sum_{e_{S_i} \in \mathcal{B}'} \mathrm{H}\left(C \mid A_{e_j}, B_{e_{S_i}} : j \notin S_i\right)$$

$$- \sum_{i \in [m]} \mathrm{I}\left(C; A_{[e_m]-e_i}\right) - \sum_{e_{S_h} \in \mathcal{B}', i \notin S_h.} \mathrm{I}\left(C; A_{e_j}, B_{e_{S_h}} : j \notin S_h, j \neq i\right)$$

$$- \sum_{e_{S_i} \in \mathcal{B}'} \mathrm{I}\left(C; A_{e_j}, B_{e_{S_i}} : j \in S_i\right) - \mathrm{I}\left(C; A_{e_i}, B_{e_{S_j}} : e_i \in \mathcal{B}'', e_{S_j} \in \mathcal{B}'\right) \leq \mathrm{H}\left(\hat{C}\right)$$

$$\leq \frac{1}{1 + \sum_i |\mathcal{B}_{e_i}|} \sum_i |\mathcal{B}_{e_i}| \, \mathrm{H}\left(A_{e_i}\right).$$

To prove the second inequality, let $k \in [m]$ such that $e_{S_k} \in \mathcal{B}'$ and let $\mathbb{F}$ be a finite field whose characteristic divides t. Let

$$C^{[0]} := C \cap \mathcal{B} \cap A_{[e_n]} \cap \left[\bigcap_{e_{S_i} \in \mathcal{B}'} \left(\sum_{j \notin S_i} A_{e_j} + B_{e_{S_i}}\right)\right].$$

We can apply to $C^{[0]}$ the same argument applied to space $C^{\langle 0 \rangle}$ in the proof of the previous inequality, we therefore obtain a subspace $C^{\{0\}} := C^{(|\mathcal{B}'|)}$. Recursively, for $i \in [m]$, we denote by $C^{\{i\}}$, a subspace of $C^{\{i-1\}}$ which is a complementary subspace to

$$\left(\sum_{e_{S_j} \in \mathcal{B}', j \neq i} B_{e_{S_j}}\right) + \left(\sum_{e_j \in \mathcal{B}'', j \neq i} A_{e_j}\right)$$

in

$$C^{\{i-1\}} + \left(\sum_{e_{S_j} \in \mathcal{B}', j \neq i} B_{e_{S_j}}\right) + \left(\sum_{e_j \in \mathcal{B}'', j \neq i} A_{e_j}\right);$$

we have

$$\mathrm{H}\left(C^{\{i-1\}} \mid C^{\{i\}}\right) \leq \mathrm{I}\left(C; A_{e_j}, B_{e_{S_i}} : e_{S_j} \in \mathcal{B}', e_j \in \mathcal{B}'', j \neq i\right)$$

We define $\tilde{C} := C^{\{m\}}$. We note that $\tilde{C} \leq \mathcal{B}$ and $\tilde{C} \cap \mathcal{B}_Y = O$, for all B_Y (where $\mathcal{B}_Y$ is the sum of all vector subspaces indexed by the columns of the submatrix B_Y of B), and the

following inequality is true

$$\mathrm{H}\left(C \mid \tilde{C}\right) = \mathrm{H}\left(C \mid C^{\{0\}}\right) + \mathrm{H}\left(C^{\{0\}} \mid \tilde{C}\right)$$

$$\leq \mathrm{H}\left(C \mid A_{e_i}, B_{e_{S_j}} : e_i \in \mathcal{B}'', e_{S_j} \in \mathcal{B}'\right) + \mathrm{H}\left(C \mid A_{[e_m]}\right) + \sum_{e_{S_i} \in \mathcal{B}'} \mathrm{H}\left(C \mid A_{e_j}, B_{e_{S_i}} : j \notin S_i\right)$$

$$+ \sum_i \mathrm{I}\left(C; A_{[e_m]-e_i}\right) + \sum_{e_{S_h} \in \mathcal{B}', i \notin S_h.} \mathrm{I}\left(C; A_{e_j}, B_{e_{S_h}} : j \notin S_h, j \neq i\right)$$

$$+ \sum_{e_{S_i} \in \mathcal{B}'} \mathrm{I}\left(C; A_{e_j}, B_{e_{S_i}} : j \in S_i\right) + \sum_i \mathrm{I}\left(C; A_{e_j}, B_{e_{S_i}} : e_{S_j} \in \mathcal{B}', e_j \in \mathcal{B}'', j \neq i\right). \quad (3.1.3)$$

The vector subspaces $A_{e_1}, \ldots, A_{e_m}$, $B_{e_{S_{j_1}}}, \ldots, B_{e_{S_{j_{|\mathcal{B}'|}}}}$ and $\tilde{C}$ satisfy hypothesis in Lemma 3.1.10. Thus,

$$\left[1 + \sum_i |\mathcal{B}_{e_i}|\right] \mathrm{H}\left(\tilde{C}\right) \leq \sum_i |\mathcal{B}_{e_i}| \, \mathrm{H}\left(A_{e_i}\right) + \mathrm{H}\left(\ker\left(\varphi_B\right)\right). \quad (3.1.4)$$

On the other hand, as B is singular over fields whose characteristic divides t, without loss generality, we suppose that there exists a submatrix B_X such that e_{S_k} is a linear combination of the columns of B_X. So, from Corollary 3.1.12,

$$\mathrm{H}\left(\ker\left(\varphi_B\right)\right) \leq \mathrm{I}\left(B_{e_{S_k}}; A_{e_i}, B_{e_{S_i}} : e_i \in B_X \cap \mathcal{B}'', e_{S_i} \in B_X \cap \mathcal{B}'\right).$$

From Lemma 3.1.1 taking $W = \tilde{C}$, $X_i = A_{e_i}$ or $X_i = B_{e_{S_i}}$ according to $e_i \in B_X \cap \mathcal{B}''$ or $e_{S_i} \in B_X \cap \mathcal{B}'$, we obtain

$$\mathrm{H}\left(\tilde{C}\right) + \mathrm{I}\left(B_{e_{S_k}}; A_{e_i}, B_{e_{S_i}} : e_i \in \mathcal{B}'', e_{S_i} \in \mathcal{B}', i \neq k\right) \leq \mathrm{H}\left(B_{e_{S_k}}\right) \text{ [we note that } X'_k \cap \mathcal{B}_X = O]$$

which implies

$$\mathrm{H}\left(\tilde{C}\right) + \mathrm{I}\left(B_{e_{S_k}}; A_{e_i}, B_{e_{S_i}} : e_i \in B_X \cap \mathcal{B}'', e_{S_i} \in B_X \cap \mathcal{B}'\right) \leq \mathrm{H}\left(B_{e_{S_k}}\right).$$

Hence, we have the inequality

$$\mathrm{H}\left(\tilde{C}\right) + \mathrm{H}\left(\ker\left(\varphi_B\right)\right) \leq \mathrm{H}\left(B_{e_{S_k}}\right).$$

Therefore, from inequality (3.1.4),

$$\left[2 + \sum_i |\mathcal{B}_{e_i}|\right] \mathrm{H}\left(\tilde{C}\right) \leq \sum_i |\mathcal{B}_{e_i}| \, \mathrm{H}\left(A_{e_i}\right) + \mathrm{H}\left(B_{e_{S_k}}\right).$$

From this and inequality (3.1.3), we obtain the desired inequality:

$$\mathrm{H}(C)-\mathrm{H}\left(C \mid A_{[e_m]}\right)-\sum_{e_{S_i}\in\mathcal{B}'}\mathrm{H}\left(C \mid A_{e_j}, B_{e_{S_i}} : j\notin S_i\right)-\mathrm{H}\left(C \mid A_{e_i}, B_{e_{S_j}} : e_i\in\mathcal{B}'', e_{S_j}\in\mathcal{B}'\right)$$

$$-\sum_i \mathrm{I}\left(C; A_{[e_m]-e_i}\right)-\sum_{e_{S_h}\in\mathcal{B}', i\notin S_h.}\mathrm{I}\left(C; A_{e_j}, B_{e_{S_h}} : j\notin S_h, j\neq i\right)$$

$$-\sum_{e_{S_i}\in\mathcal{B}'}\mathrm{I}\left(C; A_{e_j}, B_{e_{S_i}} : j\in S_i\right)-\sum_i \mathrm{I}\left(C; A_{e_j}, B_{e_{S_i}} : e_{S_j}\in\mathcal{B}', e_j\in\mathcal{B}'', j\neq i\right)$$

$$\leq \mathrm{H}\left(\tilde{C}\right)\leq \frac{1}{2+\sum\limits_i |\mathcal{B}_{e_i}|}\left(\sum_i |\mathcal{B}_{e_i}|\,\mathrm{H}(A_{e_i})+\mathrm{H}\left(B_{e_{S_k}}\right)\right).$$

□

In case that there exists i such that $A_{e_i}=O$ or $B_{e_{S_i}}=O$, then $\hat{C}=\tilde{C}=O$. We can use this to obtain that the inequalities are trivial.

Corollary 3.1.14. *If some vector space in Theorem 3.1.2 is the zero space, the inequalities implicated are linear rank inequalities.*

3.2 Two classes of inequalities

Example 3.2.1. Let $n\geq 7$ and t integer such that $2\leq t\leq \left\lfloor\frac{n-1}{2}\right\rfloor-1$ and $M(n,t)=n-t-2$. We remark that the determinant of the Matrix $B^t_{M(n,t)}$ in Figure 2.2.1 is $\pm t$. So, in Theorem 3.1.13, we take square matrices $B^t_{M(n,t)}$ with column vectors of the form $B_i := B_{e_{[M(n,t)]-i}} = c-e_i$, $A_i := A_{e_i}=e_i$, with $c=\sum\limits_{j\in[M(n,t)]} e_j$. We have:

- $\left|\det\left(B^t_{M(n,t)}\right)\right|=t$,
- $\left|\mathcal{B}'_{B^t_{M(n,t)}}\right|=t+1$,
- $\left|\mathcal{B}''_{B^t_{M(n,t)}}\right|=M(n,t)-t-1$,
- $|\mathcal{B}_{e_i}|=1$ for $i\in[t+1]$ and $|\mathcal{B}_{e_i}|=0$ for $i\in[t+2,M(n,t)]$.

Therefore, let A_1, A_2, …, $A_{M(n,t)}$, B_1, B_2, …, B_{t+1} and C be vector subspaces of a finite dimensional vector space V over a finite field $\mathbb{F}$. We have

- The following inequality is a characteristic-dependent linear rank inequality over fields whose characteristic does not divide t:

$$\mathrm{H}(C)\leq\frac{1}{t+2}\sum_{i\in[t+1]}\mathrm{H}(A_i)+\mathrm{I}\left(C; B_{[t+1]}, A_{[t+2,M(n,t)]}\right)+\mathrm{H}\left(C \mid A_{[M(n,t)]}\right)$$

$$+\sum_{i\in[M(n,t)]}\mathrm{I}\left(C;A_{[M(n,t)]-i}\right)+\sum_{i\in[t+1]}\left[\mathrm{I}\left(C;B_i\right)+\mathrm{H}\left(C\mid A_i,B_i\right)+\mathrm{I}\left(C;A_{[M(n,t)]-i},B_i\right)\right].$$

- The following inequality is a characteristic-dependent linear rank inequality over fields whose characteristic divides t:

$$\mathrm{H}\left(C\right)\leq\frac{1}{t+3}\left[\sum_{i\in[t+1]}\mathrm{H}\left(A_i\right)+\mathrm{H}\left(B_1\right)\right]+\mathrm{H}\left(C\mid B_{[t+1]},A_{[t+2,M(n,t)]}\right)+\mathrm{H}\left(C\mid A_{[M(n,t)]}\right)$$

$$+\sum_{i\in[M(n,t)]}\mathrm{I}\left(C;A_{[M(n,t)]-i}\right)+\sum_{i\in[t+1]}\left[\mathrm{I}\left(C;B_i\right)+\mathrm{H}\left(C\mid A_i,B_i\right)+\mathrm{I}\left(C;A_{[M(n,t)]-i},B_i\right)\right]$$

$$+\sum_{i\in[t+1]}\mathrm{I}\left(C;B_{[t+1]-i},A_{[t+2,M(n,t)]}\right)+\sum_{i\in[t+2,M(n,t)]}\mathrm{I}\left(C;B_{[t+1]},A_{[t+2,M(n,t)]-i}\right).$$

Remark 3.2.2. As previous chapter, we again produce a class of $\left\lfloor\frac{n-1}{2}\right\rfloor-2$ inequalities that are true over finite sets of primes and another class of $\left\lfloor\frac{n-1}{2}\right\rfloor-2$ inequalities that are true over co-finite sets of primes.

4 Applications

In this chapter, we study some linear programming problems associated to closure operators, networks and access structures. We show some application results of the inequalities obtained by the methods presented in the previous chapters.

4.1 (k, n)-Solvability problem in closure operators

Closure operators are well known in the literature. They appear in Algebra: in Group Theory as the subgroup generated by a set of elements in a group, the span of a set of vectors in Linear Algebra; in Topology as topological closure; among others [7].

Definition 4.1.1. *A closure operator on* V is a function $\mathrm{cl} : 2^V \to 2^V$ that satisfies, for all $X, Y \subseteq V$:

- $X \subseteq \mathrm{cl}(X)$.
- If $X \subseteq Y$, then $\mathrm{cl}(X) \subseteq \mathrm{cl}(Y)$.
- $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$.

The rank of cl is $r_{\mathrm{cl}} := min\{|X| : \mathrm{cl}(X) = V\}$. If there is no confusion, we write r. A basis $\mathcal{B}$ is a subset of size r whose closure is V, and a subset B that contains a basis is called spanning set.

A matroid can be thought like a closure operator which satisfies the following property:

- For any $u, v \in V$ and $X \subseteq V$, if $u \in \mathrm{cl}(X \cup v) - \mathrm{cl}(X)$, then $v \in \mathrm{cl}(X \cup u)$.

The closure operator of a matroid can be written in terms of its rank function as follows

$$\mathrm{cl}_{\mathcal{M}}(X) := \{v : r_{\mathcal{M}}(X) = r_{\mathcal{M}}(X \cup v)\}.$$

It can be proven that $\mathrm{cl}_{\mathcal{M}}$ satisfies the property mentioned above, and any closure operator, that holds the described property, defines a matroid.

Closure solvability for network coding was initially studied in [19, 20]. In [36], we study these papers. In the following, we propose a generalization or extension of the solvability problem of a closure operator. Our propose presents a problem of solvability of a closure operator on a largest class of partitions; it captures closure solvability as a particular case and can be connected to the problem of construction of fractional solutions in network coding and the problem of determining lower bounds on linear information ratios in ideal secret sharing.

Definition 4.1.2. Let B be a spanning set of cl. A (k,n)-*fractional partition solution of* cl *related to* B *over* $\mathcal{A}$ (or briefly, a (k,n)-partition solution related to B*)* is a family $\bar{\mathcal{F}} = \left(\bar{f}_v\right)_{v\in V}$ of partitions on $\mathcal{A}^{rk}$, such that

- $\left|\bar{f}_v\right| = |\mathcal{A}|^k$, if $v \in B$.
- $\left|\bar{f}_v\right| \leq |\mathcal{A}|^n$, if $v \in V - B$.
- $\left|\bar{f}_{\mathrm{cl}(X)}\right| = \left|\bar{f}_X\right|$, for all $X \subseteq V$.
- $\left|\bar{f}_V\right| = |\mathcal{A}|^{rk}$.

A basis is also a spanning set. In case that there exists a $(1,1)$-solution over $\mathcal{A}$ related to some basis $\mathcal{B}$, we say that cl is a *solvable closure operator* over $\mathcal{A}$, see [42, 19, 20, 36].

Definition 4.1.3. The *capacity* of cl (over $\mathcal{A}$ related to B) respect a class of partitions $\mathcal{D}$ is given by

$$\mathrm{C}_{\mathcal{D}}^{\mathcal{A}}(\mathrm{cl})_B := \sup\left\{\frac{k}{n} : \text{there exists a } (k,n)\text{-solution in } \mathcal{D} \text{ over } \mathcal{A} \text{ related to } \mathcal{B}\right\}.$$

We omit the subscript B when there is no confusion. The class $\mathcal{D}$ is usually taken as the class of all partitions over a power of $\mathcal{A}$, in such a case the capacity is denoted by $\mathrm{C}^{\mathcal{A}}(\mathrm{cl})$; we omit the superscript if there is no confusion. The class $\mathcal{D}$ can be also taken as the class of all kernels of linear functions over a finite field $\mathbb{F}$; in such a case, we denote $\mathrm{C}_{\mathrm{linear}}^{\mathbb{F}}(\mathrm{cl})$. Some inequalities:

$$\mathrm{C}_{\mathcal{D}}^{\mathcal{A}}(\mathrm{cl}) \leq \mathrm{C}_{\mathcal{D}}(\mathrm{cl}) \leq \mathrm{C}(\mathrm{cl}).$$

Remark 4.1.4. The entropy function of a (k,n)-fractional partition solution satisfies:

- $\mathrm{H}(v) = k$, for all $v \in B$.
- $\mathrm{H}(v) \leq n$, for all $v \in V - B$.

- $\mathrm{H}(X) = \mathrm{H}(\mathrm{cl}(X))$, for all $X \subseteq V$.
- $\mathrm{H}(V) = rk$.

Example 4.1.5. Consider the closure operator on $V = [3]$ given by

$$U_{2,3}(X) = \begin{cases} X, & \text{if } |X| \leq 2. \\ [3] & \text{otherwise.} \end{cases}$$

In $\mathcal{A} = \{0,1\}$, take $\bar{\mathcal{F}}$, the three partitions in Example 1.3.14. We have that $\bar{\mathcal{F}}$ is a $(1,1)$-partition solution related to any of its spanning sets. Hence, $U_{2,3}$ is solvable.

The following is a partial order: $\mathrm{cl}_1 \leq \mathrm{cl}_2$ if and only if $\mathrm{cl}_1(X) \subseteq \mathrm{cl}_2(X)$ for all $X \subseteq V$. We have other version of Proposition 2 in [19].

Proposition 4.1.6. *Let* cl_1 *and* cl_2 *be* r*-rank closure operators on* V*. If* $\mathrm{cl}_1 \leq \mathrm{cl}_2$ *and* cl_2 *has a* (k,n)*-partition solution related to* $\mathcal{B}$*, then* cl_1 *has the same partition solution.*

Proof. For any (k,n)-partition solution of cl_2, we have $\bar{f}_X \geq \bar{f}_{\mathrm{cl}_1(X)} \geq \bar{f}_{\mathrm{cl}_2(X)} = \bar{f}_X$ and thereby $\bar{f}_{\mathrm{cl}_1(X)} = \bar{f}_X$. It is easy to note that this family of partitions also holds the other conditions of a (k,n)-partition solution of cl_1. □

As shows the following theorem, solvable closure operator extends the concept of secret sharing matroid; not all solvable closure operator is obtained from a matroid, an example is shown in [36].

Theorem 4.1.7. *[19, Teorema 2]* $\mathrm{cl}_{\mathcal{M}}$ *is solvable over* $\mathcal{A}$ *if and only if* $\mathcal{M}$ *is a p-representable matroid over* $\mathcal{A}$*.*

4.1.1 Linear programming problems in closure operators

Let cl be a closure operator on V. We show a class of linear programming problems whose optimal solutions are upper bounds on capacities of cl. For simplicity, we write $Af \geq 0$ to mean a list A of constraints that are satisfied by a vector f. Obviously, A can be seen as a matrix.

Problem 4.1.8. *The linear programming problem of a closure operator* cl *(related to* B*) with constraint matrix* A is to determine $\max(f(V))$ for tuples of non-negative real numbers $(f(X))_{X \subseteq V}$ such that

(i) $f(v) = \frac{1}{r} f(V)$ for all $v \in \mathcal{B}$.

(ii) $f(v) \leq \frac{1}{r}$ for all $v \in V - \mathcal{B}$.

(iii) $f(X) = f(\mathrm{cl}(X))$ for all X.

(iv) $Af \geq 0$

The optimal solution is denoted by $\mathrm{B}_A(\mathrm{cl})_B$.

We are interested in adding many constraints to the matrix A in order to get better bounds. When $\bar{\mathcal{F}}$ is a (k,n)-partition solution of cl and the matrix A enumerates the constraints given by information inequalities, we can check that

$$f(X) := \frac{1}{rn}\mathrm{H}(X)$$

is a feasible solution of the linear programming problem (see Remark 4.1.4). Therefore, as $f(V) = \frac{k}{n}$ we have

$$\mathrm{C}(\mathrm{cl}) \leq \mathrm{B}(\mathrm{cl})_B := \mathrm{B}_{\text{information inequalities}}(\mathrm{cl})_B .$$

Proposition 4.1.9. *Let* cl *be a closure operator on* V*. We suppose that there exist two different basis* B_1 *and* B_2 *such that* $B_1 \cap B_2 \neq \emptyset$*. Then,* $\mathrm{C}^{\mathcal{A}}_{\mathcal{D}}(\mathrm{cl})_{B_1} \leq 1$*.*

Proof. Let f be a feasible solution of linear programming problem 4.1.8 with constraints given by information inequalities. From

$$\sum_{v\in B_1\cap B_2} f(v) + \sum_{v\in B_1 - B_2} f(v) = f(B_1) = f(B_2) \leq \sum_{v\in B_1\cap B_2} f(v) + \sum_{v\in B_2 - B_1} f(v),$$

we have

$$\frac{|B_1 - B_2|}{r} f(V) \leq \frac{|B_2 - B_1|}{r}.$$

As this works for any feasible solution and $|B_1 - B_2| = |B_2 - B_1|$, it follows that

$$\mathrm{C}^{\mathcal{A}}_{\mathcal{D}}(\mathrm{cl})_{B_1} \leq \mathrm{B}^{\mathcal{A}}_{\text{information inequalities}}(\mathrm{cl})_{B_1} \leq 1.$$

□

In case of matroids, we have the following propositions.

Corollary 4.1.10. *If* $\mathcal{M}$ *is a p-representable matroid over* $\mathcal{A}$*, then*

$$\mathrm{C}^{\mathcal{A}}(\mathcal{M}) = \mathrm{B}^{\mathcal{A}}(\mathcal{M})_B = \mathrm{B}^{\mathcal{A}}(\mathcal{M}) = 1,$$

and this capacity is achieved by a p-representation of $\mathcal{M}$ *over* $\mathcal{A}$*.*

Before continuing, we use this notation:

- $f(X \mid Y) = f(X \cup Y) - f(Y)$;
- $f(X;Y) = f(X) + f(Y) - f(X \cup Y)$.

Example 4.1.11. For any index set $\{A_1, A_2, A_3, B_1, B_2, B_3, C\}$, consider the following three constraints:

constraint (a):

$$\begin{aligned} 2f(A_1) + f(A_2) + 2f(A_3) &\leq f(B_1) + f(B_2) + f(B_3) + f(C) \\ +2f(A_1 \mid B_1, C) + f(A_2 \mid B_2, C) &+ 2f(A_3 \mid A_1, B_2) \\ +3f(B_2 \mid B_1, B_3) + 3f(C \mid A_3, B_3) &+ 5f(B_3 \mid A_1, A_2) + 5f(B_1 \mid A_2, A_3) \\ +5\left(f(A_1) + f(A_2) + f(A_3) - f(A_1, A_2, A_3)\right); & \end{aligned}$$

constraint (b):

$$\begin{aligned} f(C) \leq \frac{1}{3} f(B_1, B_2, B_3) &+ f(C \mid A_1, A_2, A_3) + f(A_2, A_3; C) \\ +f(A_1, A_3; C) + f(A_1, A_2; C) &+ f(C \mid A_1, B_1) + f(C \mid A_2, B_2) \\ +f(C \mid A_3, B_3) + f(B_1 \mid A_2, A_3) &+ f(B_2 \mid A_1, A_3) + f(B_3 \mid A_1, A_2) \\ + f(A_1; A_2, A_3) + 2f(A_1, A_2; A_3) &+ f(A_1; A_2); \end{aligned} \tag{4.1.1}$$

constraint (c):

$$\begin{aligned} f(C) \leq \frac{1}{4}\left(f(A_1) + f(A_2) + f(A_3)\right) &+ f(C \mid A_1, A_2, A_3) \\ +f(C; B_1, B_2, B_3) + f(C \mid A_1, B_1) &+ f(C \mid A_2, B_2) + f(C \mid A_3, B_3) \\ +f(C; A_2, A_3, B_1) + f(C; A_1, A_3, B_2) &+ f(C; A_1, A_2, B_3). \end{aligned}$$

From Example 1.1.6, Example 2.2.1 and Theorem 3.1.6, these constraints are true when f is the entropy function and A_1, A_2, A_3, B_1, B_2, B_3 and C are vector subspaces of a finite dimensional vector space V over a finite field $\mathbb{F}$ with characteristic other than 2. If we add to the matrix A of the linear programming problem 4.1.8, constraints given by characteristic-dependent linear rank inequalities over fields whose characteristic is 2, then we obtain a linear programming problem in which the optimal solution, denoted by $\mathrm{B}_{\mathrm{lineal}}^{\mathrm{char}(\mathbb{F})=2}(\mathrm{cl})$ is an upper bound of $\mathrm{C}_{\mathrm{lineal}}^{\mathrm{char}(\mathbb{F})=2}(\mathrm{cl})$. In analogous way, if we add the constraints given by characteristic-dependent linear rank inequalities over fields whose characteristic is other than 2 (as the

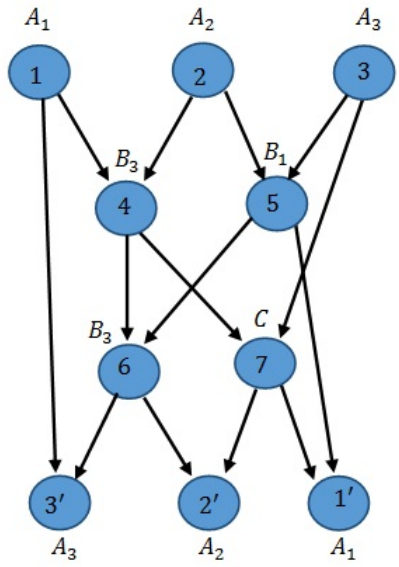

Figure 4.1.1: Fano network.

constraints (a), (b) and (c)), we obtain a linear programming problem in which the optimal solution, denoted by $\mathrm{B}_{\mathrm{lineal}}^{\mathrm{char}(\mathbb{F})\neq 2}(\mathrm{cl})$, is an upper bound of $\mathrm{C}_{\mathrm{lineal}}^{\mathrm{char}(\mathbb{F})\neq 2}(\mathrm{cl})$.

4.1.2 Applications to multiple-unicast network coding

Definition 4.1.12. Let $\mathcal{N}=(D,S,T)$ be a multiple-unicast network. The $\bar{D}$-digraph of $\mathcal{N}$ is a digraph $\bar{D}=\left(\bar{V},\bar{E}\right)$, where $\bar{V}=V$ and $\bar{E}=E\cup\{t_is_i : i=1,\ldots,r\}$.

The closure operator associated to the class of multiple-unicast networks is defined as follows.

Definition 4.1.13. Let $\mathcal{N}=(D,S,T)$ be a multiple-unicast network. For each $X\subseteq V$, let

$$\mathrm{c}_{\mathcal{N}}^{0}(X):=X,$$

$$\mathrm{c}_{\mathcal{N}}^{1}(X):=X\cup\left\{v\in V \mid v^{-}\subseteq X \text{ in } \bar{D}\right\},$$

$$\vdots$$

$$\mathrm{c}_{\mathcal{N}}^{i}(X):=\mathrm{c}_{\mathcal{N}}^{1}\left(c_{\mathcal{N}}^{i-1}(X)\right) \text{ for } 1<i\leq|V|,$$

and define $\mathrm{cl}_{\mathcal{N}}(X):=\mathrm{c}_{\mathcal{N}}^{m}(X)$. The application $\mathrm{cl}_{\mathcal{N}}:2^{V}\to 2^{V}$, that assigns $X\subseteq V$ to $\mathrm{cl}_{\mathcal{N}}(X)$, is a closure operator on V, called the closure operator of $\mathcal{N}$.

Consider the solvability problem of an operator of the form $\mathrm{cl}_{\mathcal{N}}$. In [36], we define the D^{*}digraph associated to a network deleting r-nodes of V and creating some additional edges.

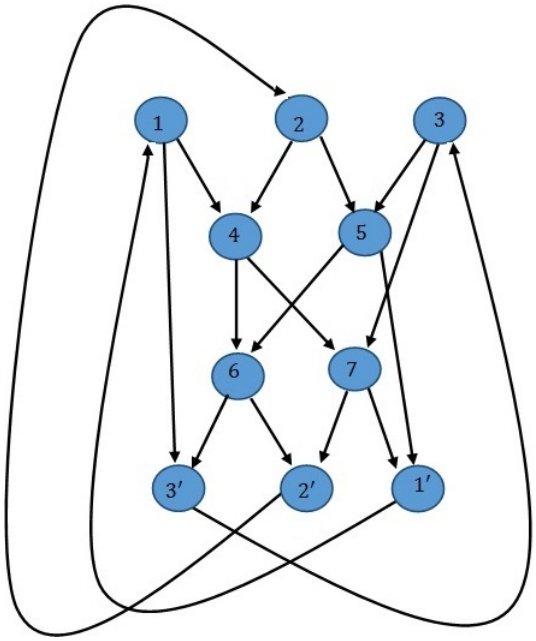

Figure 4.1.2: $\bar{D}$-digraph of the Fano network.

We then define a closure operator, denoted by cl_{D^*}. In [36, Definition 4.21], it was also given a reduction of cl_{D^*} denoted by $\mathrm{cl}^*_{D^*}$. It is straightforward to show that $\mathrm{cl}^*_{D^*} = \mathrm{cl}^*_{\mathcal{N}}$. So, $\mathrm{cl}_{\mathcal{N}}$ is solvable if and only if cl_{D^*} is solvable. The following theorem is a stronger version about (k,n)-solvability.

Theorem 4.1.14. *Let $\mathcal{N} = (D,S,T)$ be a multiple-unicast network whose closure is a r-rank closure operator. Then, $\mathcal{N}$ has a (k,n)-fractional solution over $\mathcal{A}$ if and only if $\mathrm{cl}_{\mathcal{N}}$ has a (k,n)-partition solution related to $S \cup T$ over $\mathcal{A}$.*

Proof. With helping of Theorem 1.3.13, we can follow an analogous argument to that presented in the proof of theorem 4.22 in [36]. □

As a consequence of the previous theorem:

Corollary 4.1.15. *Let $\mathcal{N} = (D,S,T)$ be a multiple-unicast network whose closure is a r-rank closure operator. Then, $\mathcal{N}$ has a (k,n)-fractional solution over $\mathcal{A}$ if and only if $\mathrm{cl}^*_{\mathcal{N}}$ has a (k,n)-partition solution related to S over $\mathcal{A}$.*

The optimal solution of the linear programming problem 4.1.8 for a closure operator of a multiple-unicast network is an upper bound on the capacity of the network over codes that hold (v):

Corollary 4.1.16. *Let $\mathcal{N} = (D,S,T)$ be a multiple-unicast network that holds the hypothesis of previous theorem. Then, $\mathrm{C}_{\mathcal{D}}(\mathcal{N}) \leq \mathrm{B}_A(\mathrm{cl}_{\mathcal{N}})$, where $\mathcal{D}$ is the class of codes that holds constraint of A.*

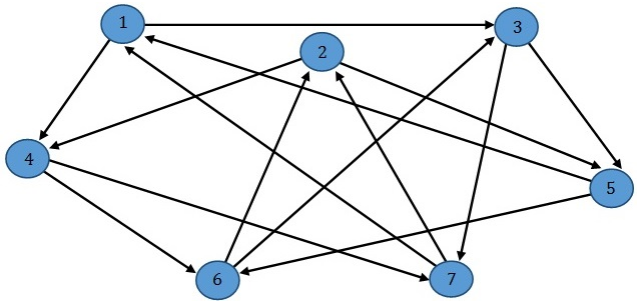

Figure 4.1.3: D^*-digraph of the Fano network.

The following proposition was proven in [11, Lemma II.1]. Here we show a proof using closure operators.

Corollary 4.1.17. *Let $\mathcal{N} = (D, S, T)$ be a multiple-unicast network such that there exists an unique path form some source s_i to receiver t_i. Then, $\mathrm{C}_{\mathcal{D}}(\mathcal{N}) \leq 1$.*

Proof. Let v_j be an member different to s_i and t_i of the mentioned path. It is enough to take $B_1 = S$, $B_2 = (S - s_i) \cup v_j$ and $\mathrm{cl} = \mathrm{cl}_{\mathcal{N}}$ in Proposition 4.1.9. We emphasize that the uniqueness of the path guarantees that $s_i \in \mathrm{cl}(B_2)$. □

We show some examples in which we use some characteristic-dependent linear rank inequalities. The main purpose is to show that the problem of fractional solvability of a closure operator is not trivial and future research can be generated.

Example 4.1.18. Consider the Fano network, Figure 4.1.1. In Figure 4.1.2 is shown its $\bar{D}$-digraph and in Figure 4.1.3 is shown its D^*-digraph. It is known that $\mathrm{C}_{\mathrm{linear}}^{\mathrm{char}(\mathbb{F})=2}(\text{Fano network}) = \mathrm{C}(\text{Fano network}) = 1$, $\mathrm{C}_{\mathrm{linear}}^{\mathrm{char}(\mathbb{F})\neq 2}(\text{Fano network}) = \frac{4}{5}$, and all these capacities are achieved by suitable solutions. We remark that Characteristic-dependent linear rank inequality, over fields whose characteristic is not 2, in Example 1.1.6 implies directly the upper bound $\frac{4}{5}$ on the linear capacity of the Fano network over fields whose characteristic is other than 2 [14]. In [11] is shown a $(4, 5)$-linear solution over field whose characteristic is different to 2. Using Theorem 4.1.14, we have $\mathrm{C}_{\mathrm{linear}}^{\mathrm{char}(\mathbb{F})=2}(\mathrm{cl}_{\text{Fano network}})_B = \mathrm{C}(\mathrm{cl}_{\text{Fano network}})_B = 1$, $\mathrm{C}_{\mathrm{linear}}^{\mathrm{char}(\mathbb{F})\neq 2}(\mathrm{cl}_{\text{Fano network}})_B = \frac{4}{5}$, when we consider the basis $B = \{A_1, A_2, A_3\}$. We also remark that we can use the linear programming problem 4.1.8 associated to the basis $\{A_1, A_2, A_3\}$ with the constraint (a) in Example 4.1.11 to get directly the upper bound $\frac{4}{5}$, and this bound is not imply directly by this constraint if we change the basis of problem of fractional solvability. In effect, $f(A_1) = f(A_2) = f(A_3) = \frac{1}{3}f(A_1, A_2, A_3) = \frac{1}{3}f(A_1, A_2, A_3, B_1, B_2, B_3, C)$, $f(B_1), f(B_2), f(B_3), f(C) \leq \frac{1}{3}$, $f(A_1 \mid B_1, C) = f(A_2 \mid B_2, C) = f(A_3 \mid A_1, B_2) = 0$, $f(B_2 \mid B_1, B_3) = f(C \mid A_3, B_3) = f(B_3 \mid A_1, A_2) = f(B_1 \mid A_2, A_3) = 0$, then substituting

these values in constraint (a), we have the inequality $\frac{5}{3}f(A_1, A_2, A_3, B_1, B_2, B_3, C) \leq \frac{4}{3}$. Hence, $\mathrm{B}_{\mathrm{linear}}^{\mathrm{char}(\mathbb{F})\neq 2}(\mathrm{cl}_{\text{Fano network}}) \leq \frac{4}{5}$. Therefore, we have a non-trivial fractional partition solution of a closure operator and our linear programming problem can prove that this solution is achievable.

We study the capacity of the Fano matroid (as closure operator) over fields where it is not representable:

Example 4.1.19. We remark that $\mathrm{cl}_{\text{Fanonetwork}} \lneqq \mathrm{cl}_{\text{Fanomatroid}}$. We have the equations $\mathrm{C}(\mathrm{cl}_{\text{Fanomatroid}})_B = \mathrm{C}_{\mathrm{lineal}}^{\mathrm{char}(\mathbb{F})=2}(\mathrm{cl}_{\text{Fanomatroid}})_B = 1$, where $B = \{A_1, A_2, A_3\}$, because the Fano matroid is p-representable over fields with characteristic 2. We can ask the value $\mathrm{C}_{\mathrm{lineal}}^{\mathrm{char}(\mathbb{F})\neq 2}(\mathrm{cl}_{\text{Fanomatroid}})_B$. As Fano matroid also satisfied the constraints of the Fano network, we have that $\mathrm{C}_{\mathrm{lineal}}^{\mathrm{char}(\mathbb{F})\neq 2}(\mathrm{cl}_{\text{Fanomatroid}}) \leq \frac{4}{5}$. We note that the $(4,5)$-partition solution that was mentioned in above example does not work for the solvability problem of the Fano matroid. In effect, a reason is that the accumulation functions $f_{A_1}^*$ and $f_{B_1}^*$ cannot determine the accumulation function f_C^* (in other words, the message of C does not be derived from the messages of $A_1$and B_1). This implies that $\bar{f}_{A_1,B_1} \neq \bar{f}_{\mathrm{cl}(A_1,B_1)}$. We want to recall that using constraints (b) and (c) in Example 4.1.11 , we get the upper bounds $\frac{8}{9}$ and $\frac{20}{21}$, respectively; they are not obviously achievable. A lower bound on $\mathrm{C}_{\mathrm{lineal}}^{\mathrm{char}(\mathbb{F})\neq 2}(\mathrm{cl}_{\text{Fanomatroid}})$ is $\frac{1}{3}$ and this is obtained by a suitable repetition code of the Fano network (it works in this case).

4.2 Parameters in index coding and network coding

Definition 4.2.1. Let m be a natural number. A *m-index coding-network* is a network with sources S and receivers T and a collection $[m]$ of m-intermediate nodes called m-block such that $S \times [m]$,$[m] \times T \subseteq E$.

The network in case $m = 1$ is simply called index coding-network and corresponds to the index coding instance studied in [4, 2]. In this case, the set of messages indexed by nodes of $t^- \cap S$ is known as the additional information of t. The message carried on intermediate node is called broadcast message. In Figure 4.2.1 is shown a general model of the digraph of an index-coding network. We remark that the network is completely determined by (S, E^*), where $E^* := \{(\tau(t), t^- \cap S) \in E : t \in T\}$. To refer to these networks, we write $\mathcal{N} = (S, E^*)$. From this, it is easy to obtain other m-index coding network $\mathcal{N}[m] = (S, E)$, letting $E = (S \times [m]) \cup ([m] \times T) \cup E^*$. The relationship between $\mathcal{N}$ and $\mathcal{N}[m]$ is established by the following lemma.

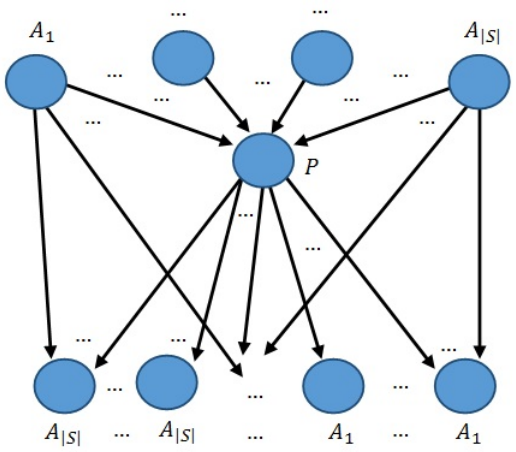

Figure 4.2.1: Index coding-network model.

Lemma 4.2.2. *Let $m \in \mathbb{N}$. A (k,n)-solution of index coding-network $\mathcal{N}$, implies a (mk,n)-solution of $\mathcal{N}[m]$. Indeed, $\mathrm{C}_{\mathcal{D}}(\mathcal{N}[m]) = m\mathrm{C}_{\mathcal{D}}(\mathcal{N})$, where $\mathcal{D}$ can be the collection of all the codes or linear codes.*

The broadcast rate for an index coding instance is defined in [2]; this parameter is used as measure of efficiency of transitions in index coding. It is known that it coincides with the inverse multiplicative of the capacity of the index coding network associated to the instance. In the following, we show some results from [5] in our network coding context.

Definition 4.2.3. Let $\mathcal{N}$ be an index coding-network, the following is a closure operator on S associated to $\mathcal{N}$, for each $Z \subseteq S$,

$$\mathrm{c}^0(Z) := Z,$$

$$\mathrm{c}^1(Z) := Z \cup \{s \in S : \exists\,(s,Y) \in E^*, Y \subseteq Z\},$$

$$\vdots$$

$$\mathrm{c}^i(Z) := \mathrm{c}^1\left(c^{i-1}(Z)\right) \text{ for } 1 < i \leq |S|,$$

we define $\mathrm{cl}(Z) := \mathrm{c}^{|S|}(Z)$.

Example 4.2.4. The butterfly network (Figure 1.3.1) is an index coding network. Its closure operator cl is equal to $U_{1,2}$; we note that the closure operator in previous section is different and equals to $U_{2,3}$ because these constructions are not the same.

4.2.1 Linear programming problems in index coding-networks

We use the following linear program problems [5]: Let $\mathcal{N} = (S, E^*)$ be an index coding-network. Consider a (k, n)-solution of $\mathcal{N}$ over $\mathcal{A}$. Let $X_1, \ldots, X_{|S|}$ be independent uniformly distributed random variables (associated to messages) over $\mathcal{A}^k$ and P be a random variable (associated to broadcast message) over $\mathcal{A}^n$. Take the base of the entropy function as $|\mathcal{A}|^k$. We have that the following conditions hold:

(i) $\mathrm{H}\left(X_1, \ldots, X_{|S|}, P\right) = |S|$,

(ii) $\mathrm{H}\left(X_i : i \in Y \mid X_j, P : j \in Z\right) \leq |Y - \mathrm{cl}\left(Z\right)|$, for all $Y \subseteq Z$.

Therefore, the entropic vector $\left(\mathrm{H}\left(X_Y, P\right)\right)_{(f(Y))}$ is a feasible solution of the following linear programming problem associated to $\mathcal{N}$.

Problem 4.2.5. *The linear programming problem* of an index coding-network $\mathcal{N}$ is to determine $\min f\left(\emptyset\right)$ for tuples of non-negative real numbers $\left(f\left(Y\right)\right)_{Y \subseteq S}$ such that

(i) $f\left(S\right) = |S|$,

(ii) $\forall Z \subseteq Y \ f\left(Y\right) - f\left(Z\right) \leq |Y - \mathrm{cl}\left(Z\right)|$,

(iii) $f\left(Y \cup Z\right) + f\left(Y \cap Z\right) \leq f\left(Y\right) + f\left(Z\right)$ for all Y, Z.

The optimal solution is denoted by $\mathrm{b}\left(\mathcal{N}\right)$. The inverse multiplicative of this value is denoted[1] by $\mathrm{B}\left(\mathcal{N}\right)$.

We have that B is an upper bound on the capacity of $\mathcal{N}$ because $f\left(\emptyset\right) \leq \mathrm{H}\left(P\right) \leq \frac{n}{k}$, yielding $\mathrm{C}\left(\mathcal{N}\right) \leq \mathrm{B}\left(\mathcal{N}\right)$. When we study the network coding problem of a network on a determined class of codes, we can modify the linear programming problem to obtain bounds on the capacity of the network over those codes. We are interesting in the class of linear codes over specific fields. So, we can add constraints associated to (characteristic-dependent) linear rank inequalities in the item (iii) of the linear programming problem 4.2.5. For simplicity, we again write $Af \geq 0$ to mean a list A of constraints that are satisfied by the vector f.

Problem 4.2.6. *The linear programming problem with constraint matrix* A of an index coding-network $\mathcal{N}$ is to determine $\min f\left(\emptyset\right)$ for tuples of non-negative real numbers $\left(f\left(Y\right)\right)_{Y \subseteq S}$ such that

(i) $f\left(S\right) = |S|$,

[1] in case $\mathrm{b} = 0$, $\mathrm{B} = \infty$.

(ii) $\forall Z \subseteq Y \ f(Y) - f(Z) \leq |Y - \mathrm{cl}(Z)|$,

(iii) $Af \geq 0$.

The optimal solution is denoted by $\mathrm{b}_A(\mathcal{N})$. The inverse multiplicative of this value is denoted by $\mathrm{B_A}(\mathcal{N})$.

We remark that when A enumerates the constraints correspond to (Shannon or non-Shannon) information inequalities, $\mathrm{B_A}$ is an upper bound on the capacity of $\mathcal{N}$; when A enumerates the constraints correspond to (characteristic-dependent) linear rank inequalities, $\mathrm{B_A}$ is an upper bound on the linear capacity of $\mathcal{N}$ over the alphabets in which the linear rank inequalities are valid.

Definition 4.2.7. A linear inequality $\sum_{i=1}^{k} \alpha_i v_{I_i} \geq 0$, $I_i \subseteq [n]$, is said to be *tight*, if for all j, we have $\sum_{j \in I_i} \alpha_i = \sum_{i=1}^{k} \alpha_i = 0$.

For any linear inequality $\sum_{i=1}^{k} \alpha_i v_{I_i} \geq 0$, let r_j be the jth residual weight, $\sum_{j \in I_i} \alpha_i$, and r_w be the residual weight, $\sum_{i=1}^{k} \alpha_i$. By definition, a tight information inequality is a *balanced information inequality* ($r_j = 0$, for all j) [9]. The proof of the following theorem is a combination of the proofs of [5, Lemma 6.3] and [9, Theorem 1].

Theorem 4.2.8. *An inequality of the form*

$$\sum_{i=1}^{k} \alpha_i \mathrm{H}(X_j : j \in I_i) \geq 0 \tag{4.2.1}$$

is a characteristic-dependent (or characteristic-independent) linear rank inequality if and only if the inequality

$$\sum_{i=1}^{k} \alpha_i \mathrm{H}(X_j : j \in I_i \mid P) - \sum_i r_i \mathrm{H}(X_i \mid X_j, P : j \in [n] - i) \geq 0 \tag{4.2.2}$$

is a tight characteristic-dependent (or characteristic-independent) linear rank inequality and $r_j, r_w \geq 0$ for all j.

Proof. Let $\mathbb{F}$ be a finite field. We suppose that the inequality (4.2.2) is true over $\mathbb{F}$. As $r_j \geq 0$, we get $\sum_i r_i \mathrm{H}(X_i \mid X_j, P : j \in [n] - i) \geq 0$. Therefore, $\sum_{i=1}^{k} \alpha_i \mathrm{H}(X_j : j \in I_i \mid P) \geq 0$ and taking $P = O$, this implies that the inequality (4.2.1) is true over $\mathbb{F}$. Reciprocally, we

suppose that the inequality (4.2.1) is true over $\mathbb{F}$. Then, it is not hard to show that the inequality is tight. Also, fixed h, when we take n vector spaces of the form

$$X_i := \begin{cases} \langle 1 \rangle, & i = h. \\ O, & \text{otherwise.} \end{cases}$$

We have

$$\mathrm{H}\left(X_j : j \in I_i\right) = \begin{cases} 1, & h \in I_i. \\ 0, & \text{otherwise.} \end{cases}$$

Therefore, from inequality (4.2.1), we obtain that

$$r_h = \sum_{h \in I_i} \alpha_i \geq 0.$$

When we take $X_i := \langle 1 \rangle$ for all i, we obtain that $r_w = \sum_{i=1}^{k} \alpha_i \geq 0$. It remains to prove that the inequality (4.2.2) is true. In [5, Lemma 6.3], it is given a linear mapping

$$\begin{aligned} B : \mathbb{R}^{2^{[n+1]}} &\to \mathbb{R}^{2^{[n]}} \\ v_J &\mapsto v_I \end{aligned}$$

with the property that each linear entropic vector in $n+1$ variables over $\mathbb{F}$ is assigned to a linear entropic vector in n variables over $\mathbb{F}$. Let α be the vector of coefficients of the inequality (4.2.1), we remark that

$$0 \leq \alpha^T B v_J = \left(B^T \alpha\right)^T v_J =: \beta^T v_J,$$

i.e. the vector β gives the coefficients of a linear inequality in $n+1$ variables over $\mathbb{F}$. We affirm that β coincides with the coefficients of the inequality (4.2.2). For commodity, we describe B^T as follows $B^T = B_{n+1} B_n \cdots B_1$, where

$$(B_i)_{ST} := \begin{cases} 1, & S = T \subsetneq [n]. \\ 1, & S = [n] - i \text{ and } i \in T. \\ -1, & S = [n] \text{ and } i \in T. \\ 0, & \text{otherwise.} \end{cases}$$

and

$$(B_{n+1})_{ST} := \begin{cases} 1, & S = T \cup n+1. \\ -1, & S = n+1. \\ 0, & \text{otherwise.} \end{cases}$$

We note that $B_1\alpha$ gives the inequality:

$$\sum_{i=1}^{k} \alpha_i \mathrm{H}\left(X_j : j \in I_i\right) - r_1 \mathrm{H}\left(X_1 \mid X_j : j \in [2,n]\right) \geq 0.$$

By induction, after applying B_n, we get the inequality:

$$\sum_{i=1}^{k} \alpha_i \mathrm{H}\left(X_j : j \in I_i\right) - \sum_i r_i \mathrm{H}\left(X_i \mid X_j : j \in [n]-i\right) \geq 0.$$

By last, we applying B_{n+1} to get the desired inequality. □

Definition 4.2.9. The *lexicographic product* of index coding networks $\mathcal{N}_1$ and $\mathcal{N}_2$, denoted by $\mathcal{N}_1 \bullet \mathcal{N}_2$, is a index coding network whose source set is $S_1 \times S_2$. Each receiver t is indexed by a pair (t_1, t_2) of receivers of $\mathcal{N}_1$ and $\mathcal{N}_2$ such that $\tau(t) = (\tau(t_1), \tau(t_2))$ and

$$t^- \cap (S_1 \times S_2) = \left[\left(t_1^- \cap S_1\right) \times S_2\right] \cup \left[\tau(t_1) \times \left(t_2^- \cap S_2\right)\right].$$

The *k-fold lexicographic power of* $\mathcal{N}$ is denoted by $\mathcal{N}^{\bullet k}$.

The broadcast rate in index coding is sub-multiplicative under lexicographic product [5, Theorem 2.2]. So, we have that the capacity of index coding-networks is super-multiplicative.

Proposition 4.2.10. *The capacity of index coding-networks is super-multiplicative under lexicographic product, i.e.,* $\mathrm{C}(\mathcal{N}_1)\,\mathrm{C}(\mathcal{N}_2) \leq \mathrm{C}(\mathcal{N}_1 \bullet \mathcal{N}_2)$.

From [5, Theorem 1.1], as the optimal solution b_A is super-multiplicative under the lexicographic products, B_A is sub-multiplicative:

Theorem 4.2.11. *Add in the item (iii) of the linear programming problem 4.2.6 constraints given by tight characteristic dependent (or characteristic-independent) linear rank inequalities. Then, the optimal solution* B_A *is sub-multiplicative under lexicographic products.*

Example 4.2.12. [5] The submodular inequality can be replaced by the following tight inequality $f(A \cup B \cup C) + f(C) \leq f(A \cup C) + f(B \cup C)$. The optimal solution B is sub-multiplicative under lexicographic products i.e., $\mathrm{B}(\mathcal{N}_1 \bullet \mathcal{N}_2) \leq \mathrm{B}(\mathcal{N}_1)\,\mathrm{B}(\mathcal{N}_2)$.

Remark 4.2.13. Let $t \in \mathbb{N}$, $t \geq 2$. In Example 2.2.1, taking $n = 2t+3$, we have the following two classes of characteristic-dependent linear rank inequalities:

(a) If $\mathrm{char}(\mathbb{F})$ divides t,

$$\mathrm{H}\left(B_{[t+1]}\right) \leq t\mathrm{I}\left(A_{[t+1]}; C\right) + [t+1]\left(\mathrm{H}\left(C \mid A_{[t+1]}\right) + \sum_{i=1}^{t+1} \mathrm{I}\left(A_{[t+1]-i}; C\right)\right)$$

$$+\sum_{i=1}^{t+1}\left(\mathrm{H}\left(B_i \mid A_i, C\right)+\mathrm{H}\left(B_i \mid A_{[t+1]-i}\right)+\mathrm{I}\left(A_{[i]}; A_{[i+1,t+1]}\right)+\mathrm{I}\left(A_{[i-1]}; A_i\right)\right).$$

(b) If $\mathrm{char}\left(\mathbb{F}\right)$ does not divide t,

$$\mathrm{H}\left(C\right) \leq \frac{1}{t+1}\mathrm{H}\left(B_{[t+1]}\right)+\mathrm{H}\left(C \mid A_{[t+1]}\right)+\sum_{i=1}^{t+1}\mathrm{I}\left(A_{[t+1]-i}; C\right)$$

$$+\sum_{i=1}^{t+1}\left(\mathrm{H}\left(C \mid A_i, B_i\right)+\mathrm{H}\left(B_i \mid A_{[t+1]-i}\right)+\mathrm{I}\left(A_{[i]}; A_{[i+1,t+1]}\right)+\mathrm{I}\left(A_{[i-1]}; A_i\right)\right).$$

We want to define linear programming problems, using these inequalities, whose solutions behave super-multiplicatively under lexicographic products. We apply theorem 4.2.8 to get two tight characteristic-dependent linear rank inequalities:

Proposition 4.2.14. *For any A_1, A_2, …, A_{t+1}, B_1, B_2, …, B_{t+1}, C and P vector subspaces of V, we get*

$$\mathrm{H}\left(B_{[t+1]} \mid P\right)+\sum_{i=1}^{t+1}\mathrm{H}\left(B_i \mid A_{[t+1]}, B_{[t+1]-i}, C, P\right)+(t+1)\,\mathrm{H}\left(C \mid A_{[t+1]}, B_{[t+1]}, P\right)$$

$$\leq t\mathrm{I}\left(A_{[t+1]}; C \mid P\right)+[t+1]\left(\mathrm{H}\left(C \mid A_{[t+1]}, P\right)+\sum_{i=1}^{t+1}\mathrm{I}\left(A_{[t+1]-i}; C \mid P\right)\right)$$

$$+\sum_{i=1}^{t+1}\left(\mathrm{H}\left(B_i \mid A_i, C, P\right)+\mathrm{H}\left(B_i \mid A_{[t+1]-i}, P\right)+\mathrm{I}\left(A_{[i]}; A_{[t+1]-[i]} \mid P\right)+I\left(A_{[i-1]}; A_i \mid P\right)\right) \tag{4.2.3}$$

when $\mathrm{char}\left(\mathbb{F}\right)$ divides t;

$$\mathrm{H}\left(C \mid P\right)+(t+1)\,\mathrm{H}\left(C \mid A_{[t+1]}, B_{[t+1]}, P\right)+\frac{t+2}{t+1}\sum_{i=1}^{t+1}\mathrm{H}\left(B_i \mid A_{[t+1]}, B_{[t+1]-i}, C, P\right)$$

$$\leq \frac{1}{t+1}\mathrm{H}\left(B_{[t+1]} \mid P\right)+\mathrm{H}\left(C \mid A_{[t+1]}, P\right)+\sum_{i=1}^{t+1}\mathrm{I}\left(A_{[t+1]-i}; C \mid P\right)$$

$$+\sum_{i=1}^{t+1}\left(\mathrm{H}\left(C \mid A_i, B_i, P\right)+\mathrm{H}\left(B_i \mid A_{[t+1]-i}, P\right)+\mathrm{I}\left(A_{[i]}; A_{[t+1]-[i]} \mid P\right)+\mathrm{I}\left(A_{[i-1]}; A_i \mid P\right)\right) \tag{4.2.4}$$

when $\mathrm{char}\left(\mathbb{F}\right)$ does not divide t.

Proof. Fixed t, we apply Theorem 4.2.8 to the two inequalities in previous remark. We note that $r_{A_i} = 0$ for all i, $r_{B_i} = 1$ for all i, $r_C = t+1$ and $r_w = t^2+5t+2$ in the

first inequality; and $r_{A_i} = 0$ for all i, $r_{B_i} = \frac{t+2}{t+1}$ for all i, $r_C = t+1$ and $r_w = \frac{3t^2+5t+3}{t+1}$ in the second inequality. In Theorem 4.2.8, an expression of the form $\mathrm{H}(X_j : j \in I)$ in a inequality is turned in a expression of the form $\mathrm{H}(X_j, P : j \in I)$ in the inequality (4.2.2). Noting that for any X, Y and P vector subspaces, the following identities hold $\mathrm{I}(X;Y \mid P) = \mathrm{H}(X \mid P) + \mathrm{H}(Y \mid P) - \mathrm{H}(X,Y \mid P)$ and $\mathrm{H}(X \mid Y,P) = \mathrm{H}(X,Y \mid P) - \mathrm{H}(Y \mid P)$, we have that an expression of the form $\mathrm{H}(X_j : j \in I \mid X_j : j \in J)$ is turned in a expression of the form $\mathrm{H}(X_j : j \in I \mid X_j, P : j \in J)$, and an expression of the form $\mathrm{I}(X_j : j \in I; X_j : j \in J \mid P)$ is turned in a expression of the form $\mathrm{H}(X_j : j \in I; X_j, P : j \in J)$. With this in mind, it is straightforward to verify that the described inequalities in this corollary coincide with the tight forms of the mentioned inequalities. □

We use these inequalities to define two new linear programming problems adding the constraints imply by each one of theses inequalities to the matrix A of LP with constraint matrix given by submodular inequality. The linear programming problem which use the first inequality, we shall call LP-$\mathcal{A}_t$, and the linear programming problem which use the second inequality, we shall call LP-$\mathcal{B}_t$. The optimal solutions are denoted by $\mathrm{b}_{\mathcal{A}_t}$ and $\mathrm{b}_{\mathcal{B}_t}$.

Corollary 4.2.15. *The following inequality is a constraint which is satisfied by LP-$\mathcal{A}_t$, this is obtained from inequality (4.2.3) and Theorem 4.2.8,*

$$\left[t^2+5t+2\right] f(\emptyset) + [t+2]\, f\left(A_{[t+1]}\right) + (t+1) \sum_{i=1}^{t+1} f\left(A_{[t+1]-i}, C\right) + f\left(B_{[t+1]}\right)$$

$$+2(t+1)\, f\left(A_{[t+1]}, B_{[t+1]}, C\right) + \sum_{i=1}^{t+1} f(A_i, C) \leq (t+1)\, f\left(A_{[t+1]}, B_{[t+1]}\right) + f\left(A_{[t+1]}, C\right)$$

$$+t \sum_{i=1}^{t+1} f\left(A_{[t+1]-i}\right) + \left(t^2+3t+1\right) f(C) + \sum_{i=1}^{t+1} \left[f(B_i, A_i, C) + f\left(B_i, A_{[t+1]-i}\right) + f\left(A_{[t+1]-[i]}\right)\right]$$

$$+ \sum_{i=1}^{t+1} \left[f\left(A_{[i-1]}\right) + f(A_i) + f\left(A_{[t+1]}, B_{[t+1]-i}, C\right)\right]; \tag{4.2.5}$$

in analogous way, the following inequality is a constraint which is satisfied by LP-$\mathcal{B}_t$, this is obtained from inequality (4.2.4) and Theorem 4.2.8,

$$\frac{3t^2+5t+3}{t+1} f(\emptyset) + (2t+3)\, f\left(C, A_{[t+1]}, B_{[t+1]}\right) + \sum_{i=1}^{t+1} f\left(A_{[t+1]-i}, C\right) + (t+2)\, f\left(A_{[t+1]}\right)$$

$$+ \sum_{i=1}^{t+1} f(A_i, B_i) \leq (t+1)\, f\left(A_{[t+1]}, B_{[t+1]}\right) + \frac{t+2}{t+1} \sum_{i=1}^{t+1} f\left(A_{[t+1]}, B_{[t+1]-i}, C\right)$$

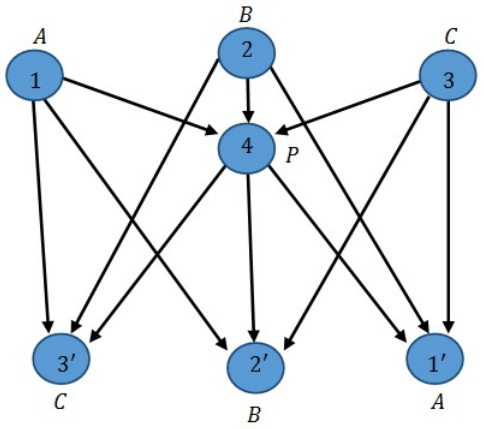

Figure 4.2.2: Index coding-network from matroid $U_{2,3}$.

$$+\frac{1}{t+1}f\left(B_{[t+1]}\right)+f\left(C,A_{[t+1]}\right)+tf\left(C\right)+\sum_{i=1}^{t+1}\left[f\left(C,A_i,B_i\right)+f\left(B_i,A_{[t+1]-i}\right)\right]$$

$$+\sum_{i=1}^{t+1}\left[f\left(A_{[t+1]-[i]}\right)+f\left(A_{[i-1]}\right)+f\left(A_i\right)\right]. \tag{4.2.6}$$

Also, the optimal solutions of our LP-problems are super-multiplicative under lexicographic products.

Proof. By Theorem 4.2.11, the optimal solutions of these problems are super-multiplicative under lexicographic products. Taking $P=\emptyset$ in item (iii) of each linear programming problem, the two described constraints are implicated . □

4.2.2 A family of index coding-networks

Let $\mathcal{M}=(S,r)$ be a matroid and let J be the set of coloops of $\mathcal{M}$ (each element is in no circuit). Consider the matroid obtained by deletion of J, $\mathcal{M}\mid J=(S-J,r\mid_J)$. *The index coding network associated to* $\mathcal{M}$ is an index coding-network, denoted by $\mathcal{N}_{\mathcal{M}}$, with source set $S-J$ and $E^*_{\mathcal{M}}:=\{(s,C-s):C \text{ is a circuit in } \mathcal{M}\mid J, s\in C\}$ .This construction is a modification of the construction given by Blasiak et al. [5, Definition 5.1]. Our network has a smaller number of sources and receivers because it is completely determined by the circuits of the matroid. In Figure 4.2.2, it is show an example of the index coding-network from matroid $U_{2,3}$. We introduce the following definition in order to study the properties of these networks.

Definition 4.2.16. An index coding network $\mathcal{N}'=(S,E^*_{\mathcal{N}'})$ is called an *index coding-subnetwork of* $\mathcal{N}$, if $E^*_{\mathcal{N}'}\subseteq E^*_{\mathcal{N}}$ and there exists a collection $\{(s,S_s)\}_{s\in S}$ of elements of $E^*_{\mathcal{N}'}$

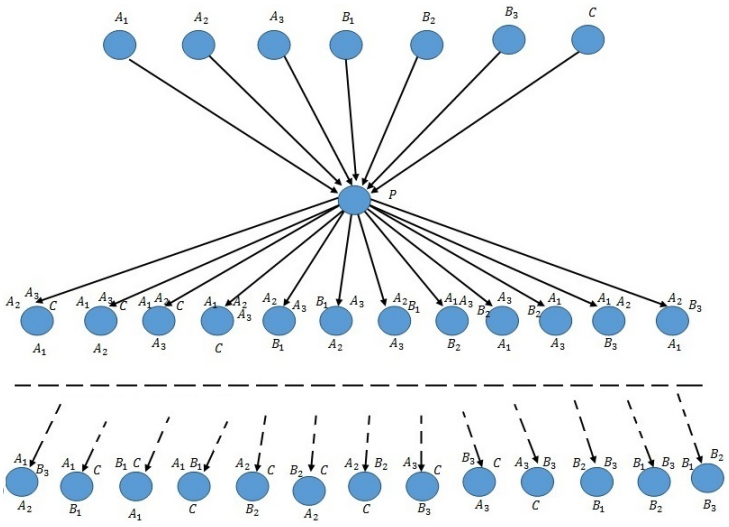

Figure 4.2.3: Fano index coding-network

such that $T := \bigcup_{s \in S} S_s$ is a minimum subset of S, with the property that for all $s \in S$, $(s, T_s) \in E^*_{\mathcal{N}}$, for some $T_s \subseteq T$.

Proposition 4.2.17. *$\mathcal{N}'$ is a index coding-subnetwork of $\mathcal{N}$ if and only if $cl_{\mathcal{N}'} \leq cl_{\mathcal{N}}$ and $r_{cl_{\mathcal{N}'}} = r_{cl_{\mathcal{N}}}$.*

The definition of subnetwork guarantees that the network flow of a subnetwork behaves like the network flow of the network. Specifically, a solution of $\mathcal{N}$ is a solution of $\mathcal{N}'$ and $\mathrm{b}(\mathcal{N}') \leq \mathrm{b}(\mathcal{N})$. Furthermore, the index coding network of a matroid $\mathcal{M}$ is an index coding-subnetwork of the index coding-network obtained from the index coding instance associated to the matroid $\mathcal{M} \mid J$ of Blasiak et al. With this in mind, the following proposition (and proof) is a rewriting of [5, Proposition 5.2 and Theorem 5.4].

Proposition 4.2.18. *Let $\mathcal{M} = (S, r)$ be a matroid. For any index coding-subnetwork $\mathcal{N}$ of the index coding network $\mathcal{N}_{\mathcal{M}}$,*

$$\mathrm{B}(\mathcal{N}) = \frac{1}{|S| - r_{\mathcal{M}}}.$$

Also, if $\mathcal{M}$ is representable over some $\mathbb{F}$, then

$$\mathrm{C}(\mathcal{N}) = \mathrm{C}^{\mathbb{F}}_{linear}(\mathcal{N}) = \frac{1}{|S| - r_{\mathcal{M}}}$$

and this capacity is achieved by a $(1, |S| - r_{\mathcal{M}})$-linear solution over $\mathbb{F}$.

4.2.2.1 Applications to network coding

$$\begin{array}{c} B_1 \cdots B_{t+1} \\ \begin{pmatrix} 0 & \cdots & 1 \\ 1 & \vdots & 1 \\ \vdots & \vdots & \vdots \\ 1 & \vdots & 1 \\ 1 & \cdots & 0 \end{pmatrix} \end{array}$$

Figure 4.2.4: Matrix $B^t_{M(2t+3,t)}$.

We use index coding-networks from matroids for proving the main theorem of this section. Fixed t and a finite field $\mathbb{F}$. The matrix L_t in Figure 4.2.4, with entries in $\mathbb{F}$, induces a representable matroid $\mathcal{M}(L_t)$ with ground set

$$S := \{A_1, \ldots, A_{t+1}, B_1, \ldots, B_{t+1}, C\},$$

some of these are known in [25] for n prime. If we change the field, it is possible that the vector matroid changed. However, these matroids have some properties in common. Specifically, certain subsets of the ground set of $\mathcal{M}(L_t)$ are always circuits according to the characteristic of $\mathbb{F}$ divides or does not t. We classify them in two types: The collection

$$\mathcal{A}_t := \left\{A_{[t+1]}C, A_{[t+1]-i}B_i, A_iB_iC, B_{[t+1]} : i \in [t+1]\right\}$$

is a subclass of circuits in any $\mathcal{M}(L_t)$ over $\mathbb{F}$, when $\mathrm{char}(\mathbb{F})$ divides t; and the collection

$$\mathcal{B}_t := \left\{A_{[t+1]}C, A_{[t+1]-i}B_i, A_iB_iC, B_{[t+1]}C : i \in [t+1]\right\}$$

is a subclass of circuits in any $\mathcal{M}(L_t)$ over $\mathbb{F}$, when $\mathrm{char}(\mathbb{F})$ does not divide t.

Definition 4.2.19. We define $\mathcal{N}_{\mathcal{A}_t}$ as the index coding with the source set S and

$$E^*_{\mathcal{A}_t} := \{(s, C-s) : C \in \mathcal{A}_t, s \in C\};$$

and $\mathcal{N}_{\mathcal{B}_t}$ as the index coding with the source set S and

$$E^*_{\mathcal{B}_t} := \{(s, C-s) : C \in \mathcal{B}_t, s \in C\}.$$

Example 4.2.20. In Figure 4.2.3, the Fano index-coding network $\mathcal{N}_{\mathcal{A}_2}$ is illustrated. In

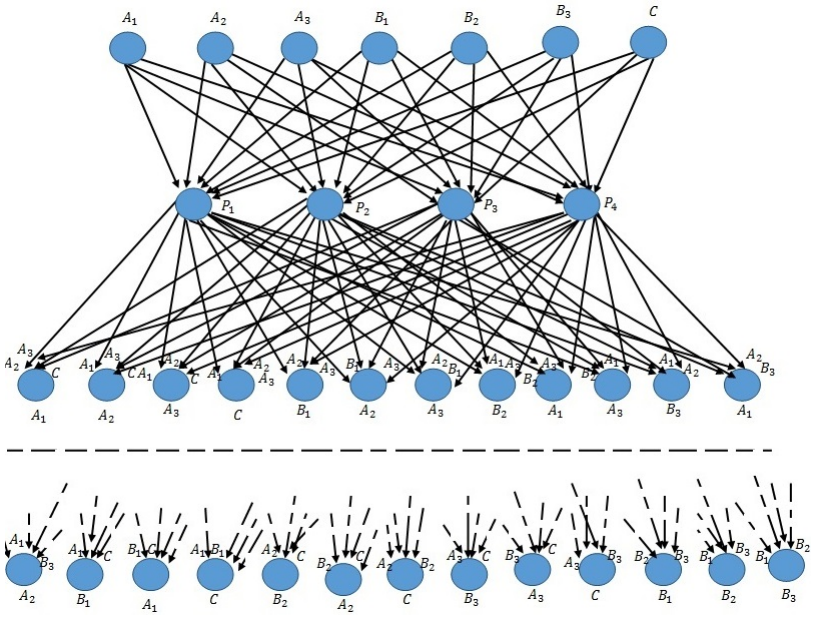

Figure 4.2.5: Solvable Fano 4-index coding-network

Figure 4.2.5, it is illustrated the network $\mathcal{N}_{\mathcal{A}_2}$ [4] obtained from $\mathcal{N}_{\mathcal{A}_2}$.

Before continuing, the following statements are useful.

Lemma 4.2.21. *For any $\mathcal{N}_1$ and $\mathcal{N}_2$. If $\mathcal{N}_1$ has a (n,m)-linear solution and $\mathcal{N}_2$ has a (k,n)-linear solution both over the same field, then $\mathcal{N}_1 \bullet \mathcal{N}_2$ has a (k,m)-linear solution.*

Proof. Let f be the function on the intermediate node and f_{t_1} be the decoding function on a receiver t_1 of the desired (n,m)-linear solution of $\mathcal{N}_1$, and let g be the function on the intermediate node and g_{t_2} be the decoding function on a receiver t_2 of the desired (k,n)-linear solution of $\mathcal{N}_2$. Define

$$g'(x) := \left(g\left(x_{s_1\times S_2}\right)\right)_{s_1\in S_1}, \text{ for } x \in \mathbb{F}^{k|S_1\times S_2|},$$

and let $h = fg'$ be the function on the intermediate node in $\mathcal{N}_1 \bullet \mathcal{N}_2$. We obtain the broadcast message $h(x) \in \mathbb{F}^m$. Let t be a receiver in $\mathcal{N}_1 \bullet \mathcal{N}_2$ such that $\tau(t) = (\tau(t_1), \tau(t_2))$ and

$$t^- \cap (S_1 \times S_2) = \left[\left(t_1^- \cap S_1\right) \times S_2\right] \cup \left[\tau(t_1) \times \left(t_2^- \cap S_2\right)\right].$$

We have

$$f_{t_1}\left(h(x), \left(g\left(x_{s_1\times S_2}\right)\right)_{s_1\in t_1^-\cap S_1}\right) = f_{t_1}\left(f\left(\left(g\left(x_{s_1\times S_2}\right)\right)_{s_1\in S_1}\right), \left(g\left(x_{s_1\times S_2}\right)\right)_{s_1\in t_1^-\cap S_1}\right)$$

$$= g\left(x_{\tau(t_1)\times S_2}\right).$$

Then,

$$g_{t_2}\left(g\left(x_{\tau(t_1)\times S_2}\right), x_{\tau(t_1)\times\left(t_2^-\cap S_2\right)}\right) = x_{(\tau(t_1),\tau(t_2))}.$$

These equations and h define a (k,m)-linear solution of $\mathcal{N}_1 \bullet \mathcal{N}_2$. □

Lemma 4.2.22. *For $k \in \mathbb{N}$. If $\mathcal{N}$ has a $(1,n)$-linear solution, then $\mathcal{N}^{\bullet k}$ has a $\left(1, n^k\right)$-linear solution.*

Proof. By induction, case $k = 2$, take $\mathcal{N}_1 = \mathcal{N}_2 = \mathcal{N}$ in Lemma 4.2.21 and note that $\mathcal{N}_2$ has a (n, n^2)-linear solution by repetition of the given solution of $\mathcal{N}$. We get a $(1, n^2)$-linear solution of $\mathcal{N}^{\bullet 2}$. Now, we suppose that case $k-1$ holds i.e. $\mathcal{N}^{\bullet k-1}$ has a $\left(1, n^{k-1}\right)$-linear solution. Take $\mathcal{N}_1 = \mathcal{N}$, $\mathcal{N}_2 = \mathcal{N}^{\bullet k-1}$ in Lemma 4.2.21 and note that $\mathcal{N}_1$ has a $\left(n^{k-1}, n^k\right)$-linear solution by repetition of the given solution of $\mathcal{N}$. Then, $\mathcal{N}^{\bullet k}$ has a $\left(1, n^k\right)$-linear solution. □

Theorem 4.2.23. *For any $k, t \in \mathbb{N}$, $t \geq 2$. We have,*

(i) $\mathcal{N}_{\mathcal{A}_t}^{\bullet k}\left[(t+2)^k\right]$ is linearly solvable over a field $\mathbb{F}$ if and only if $char(\mathbb{F})$ divides t. Also, when $char(\mathbb{F}) \nmid t$,

$$\left(\frac{t+2}{t+3}\right)^k \leq \mathrm{C}_{linear}^{\mathbb{F}}\left(\mathcal{N}_{\mathcal{A}_t}^{\bullet k}\left[(t+2)^k\right]\right) \leq \left(\frac{2t^3+9t^2+13t+6}{2t^3+9t^2+13t+7}\right)^k.$$

(ii) $\mathcal{N}_{\mathcal{B}_t}^{\bullet k}\left[(t+2)^k\right]$ is linearly solvable over a field $\mathbb{F}$ if and only if $char(\mathbb{F})$ does not divide t. Also, when $char(\mathbb{F}) \mid t$,

$$\left(\frac{t+2}{t+3}\right)^k \leq \mathrm{C}_{linear}^{\mathbb{F}}\left(\mathcal{N}_{\mathcal{B}_t}^{\bullet k}\left[(t+2)^k\right]\right) \leq \left(\frac{t^3+5t^2+9t+6}{t^3+5t^2+9t+7}\right)^k.$$

Proof. To prove (i), we have that $\mathcal{N}_{\mathcal{A}_t}$ is an index coding-subnetwork of any $\mathcal{N}_{\mathcal{M}(L_t)}$ when $\mathrm{char}\,(\mathbb{F})$ divides t. Using Lemma 4.2.18, we have

$$\mathrm{C}\left(\mathcal{N}_{\mathcal{A}_t}\right) = \mathrm{C}_{\mathrm{linear}}^{\mathbb{F}}\left(\mathcal{N}_{\mathcal{A}_t}\right) = \frac{1}{t+2},$$

when $\mathrm{char}\,(\mathbb{F})$ divides t and this capacity is achieved by a $(1, t+2)$-linear solution over $\mathbb{F}$. By Lemma 4.2.22 with $\mathcal{N} = \mathcal{N}_{\mathcal{A}_t}$, $\mathcal{N}_{\mathcal{A}_t}^{\bullet k}$ has a $\left(1, (t+2)^k\right)$-linear solution over $\mathbb{F}$. Finally, by Lemma 4.2.2, $\mathcal{N}_{\mathcal{A}_t}^{\bullet k}\left[(t+2)^k\right]$ has a $\left((t+2)^k, (t+2)^k\right)$-linear solution over $\mathbb{F}$ which implies that $\mathcal{N}_{\mathcal{A}_t}^{\bullet k}\left[(t+2)^k\right]$ is linearly solvable over a field $\mathbb{F}$ whose $\mathrm{char}\,(\mathbb{F})$ divides t. We estimate an upper bound on $\mathrm{C}_{\mathrm{linear}}^{\mathbb{F}}\left(\mathcal{N}_{\mathcal{A}_t}\right)$ when $\mathrm{char}\,(\mathbb{F})$ does not divide t, using the LP-$\mathcal{B}_t$: Let $(z_S)_{S\subseteq V}$ be a solution of LP-$\mathcal{B}_t$ for $\mathcal{N}_{\mathcal{A}_t}$. From definition of $\mathcal{N}_{\mathcal{A}_t}$, we have:

(a) If X is a dependent set in each $\mathcal{M}(L_t)$ ($\mathrm{char}(\mathbb{F})$ divides t), then

$$f(X) \leq f\left(\mathcal{B}_X^{\mathcal{M}(L_t)}\right) \leq f(\emptyset) + r_{\mathcal{M}(L_t)}(X).$$

(b) If X is an independent set in each $\mathcal{M}(L_t)$ ($\mathrm{char}(\mathbb{F})$ divides t), then

$$|X| + t + 2 \leq f(X) \leq f(\emptyset) + |X|.$$

(c) If X contains a basis, then

$$2t + 3 \leq f(X) \leq f(\mathcal{B}_X) \leq f(\emptyset) + t + 1.$$

We can use constraints implied by these conditions along with the constraint 4.2.6 to get

$$\frac{3t^2+5t+3}{t+1} f(\emptyset) + (2t+3)^2 \leq f(\emptyset) + t + 1$$

$$+\frac{1}{t+1}\left(f(\emptyset)+t\right) + t\left(f(\emptyset)+1\right) + (t+1)\left(f(\emptyset)+t\right) + (t+1)\left[3f(\emptyset)+t+1\right].$$

Simplifying,

$$f(\emptyset) \geq \frac{2t^3+9t^2+13t+7}{2t^2+5t+3},$$

which implies that

$$\mathrm{b}_{\mathcal{B}_t}(\mathcal{N}_{\mathcal{A}_t}) \geq \frac{2t^3+9t^2+13t+7}{2t^2+5t+3}.$$

Using super-multiplicative of $\mathrm{b}_{\mathcal{B}_t}$ under lexicographic products,

$$\mathrm{b}_{\mathcal{B}_t}\left(\mathcal{N}_{\mathcal{A}_t}^{\bullet k}\right) \geq \left(\frac{2t^3+9t^2+13t+7}{2t^2+5t+3}\right)^k.$$

Then

$$\mathrm{C}_{\mathrm{linear}}^{\mathbb{F}}\left(\mathcal{N}_{\mathcal{A}_t}^{\bullet k}\right) \leq \left(\frac{2t^2+5t+3}{2t^3+9t^2+13t+7}\right)^k.$$

Hence, using Lemma 4.2.2 with $m = (t+2)^k$,

$$\mathrm{C}_{\mathrm{linear}}^{\mathbb{F}}\left(\mathcal{N}_{\mathcal{A}_t}^{\bullet k}\left((t+2)^k\right)\right) \leq \left(\frac{2t^3+9t^2+13t+6}{2t^3+9t^2+13t+7}\right)^k < 1,$$

when $\mathrm{char}(\mathbb{F})$ does not divide t. To prove item (ii), we have that $\mathcal{N}_{\mathcal{B}_t}$ is an index coding-

subnetwork of any $\mathcal{N}_{\mathcal{M}(L_t)}$ when $\mathrm{char}(\mathbb{F})$ does not divide t. Using Lemma 4.2.18, we have

$$\mathrm{C}\left(\mathcal{N}_{\mathcal{B}_t}\right) = \mathrm{C}_{\mathrm{linear}}^{\mathbb{F}}\left(\mathcal{N}_{\mathcal{B}_t}\right) = \frac{1}{t+2},$$

when $\mathrm{char}(\mathbb{F})$ does not divide t and this capacity is achieved by a $(1, t+2)$-linear solution over $\mathbb{F}$. Then, we apply an argument as in (i) to get the required linear solution of $\mathcal{N}_{\mathcal{B}_t}^{\bullet k}\left[(t+2)^k\right]$. We estimate an upper bound on $\mathrm{C}_{\mathrm{linear}}^{\mathbb{F}}\left(\mathcal{N}_{\mathcal{B}_t}\right)$ when $\mathrm{char}(\mathbb{F})$ divides t using the LP-$\mathcal{A}_t$: Let $(z_S)_{S\subseteq V}$ be a solution of LP-$\mathcal{A}_t$ for $\mathcal{N}_{\mathcal{B}_t}$. From definition of $\mathcal{N}_{\mathcal{B}_t}$, we have that this network satisfies conditions (a)-(c) of part (i) when the matroid $\mathcal{M}(L_t)$ is taken over a field $\mathbb{F}$ whose $\mathrm{char}(\mathbb{F})$ does not divide t. We can use constraints implied by these conditions along with the constraint 4.2.5 to get

$$\left[t^2+5t+2\right] f(\emptyset) + t(t+1)(2t+3) + (2t+3) + 2(t+1)(2t+3) \leq$$

$$t(t+1)(f(\emptyset)+t) + \left(t^2+3t+1\right)(f(\emptyset)+1) + (t+1)\left[4f(\emptyset)+2t+1\right].$$

Simplifying,

$$f(\emptyset) \geq \frac{t^3+5t^2+9t+7}{t^2+3t+3},$$

which implies that

$$\mathrm{b}_{\mathcal{A}_t}\left(\mathcal{N}_{\mathcal{B}_t}\right) \geq \frac{t^3+5t^2+9t+7}{t^2+3t+3}.$$

Then, using super-multiplicative of $\mathrm{b}_{\mathcal{A}_t}$ under lexicographic products,

$$\mathrm{b}_{\mathcal{A}_t}\left(\mathcal{N}_{\mathcal{B}_t}^{\bullet k}\right) \geq \left(\frac{t^3+5t^2+9t+7}{t^2+3t+3}\right)^k.$$

Thus,

$$\mathrm{C}_{\mathrm{linear}}^{\mathbb{F}}\left(\mathcal{N}_{\mathcal{B}_t}^{\bullet k}\right) \leq \left(\frac{t^2+3t+3}{t^3+5t^2+9t+7}\right)^k,$$

when $\mathrm{char}(\mathbb{F})$ divide t. Hence, using Lemma 4.2.2 with $m = (t+2)^k$,

$$\mathrm{C}_{\mathrm{linear}}^{\mathbb{F}}\left(\mathcal{N}_{\mathcal{B}_t}^{\bullet k}\left((t+2)^k\right)\right) \leq \left(\frac{t^3+5t^2+9t+6}{t^3+5t^2+9t+7}\right)^k < 1,$$

when $\mathrm{char}(\mathbb{F})$ divides t.

To prove the lower bounds on the linear capacities over fields in which the networks are not linearly solvable, we use the network topology in common of $\mathcal{N}_{\mathcal{A}_t}$ and $\mathcal{N}_{\mathcal{B}_t}$: We add the message of C to the broadcast message of the $(1, t+2)$-linear solution of $\mathcal{N}_{\mathcal{B}_t}$ over $\mathbb{F}$

when $\mathrm{char}(\mathbb{F})$ does not divide t to obtain a $(1, t+3)$-linear code which is a linear solution of $\mathcal{N}_{\mathcal{A}_t}$ over this field. Then, the solution is extended to a $\left((t+2)^k, (t+3)^k\right)$-linear solution of $\mathcal{N}_{\mathcal{A}_t}^{\bullet k}\left[(t+2)^k\right]$ yielding

$$\left(\frac{t+2}{t+3}\right)^k \leq \mathrm{C}_{\mathrm{linear}}^{\mathbb{F}}\left(\mathcal{N}_{\mathcal{A}_t}^{\bullet k}\left[(t+2)^k\right]\right).$$

In an analogous way, we get the respective lower bound on $\mathrm{C}_{\mathrm{linear}}^{\mathbb{F}}\left(\mathcal{N}_{\mathcal{B}_t}^{\bullet k}\left[(t+2)^k\right]\right)$, when $\mathrm{char}(\mathbb{F})$ divides t. □

Corollary 4.2.24. *Let P be a finite or co-finite set of primes. There exists a sequence of networks $\left(\mathcal{N}_P^k\right)_k$ in which each member is linearly solvable over a field $\mathbb{F}$ if and only if the characteristic of $\mathbb{F}$ is in P. Furthermore, when $\mathrm{char}(\mathbb{F})$ is not in P, $\mathrm{C}_{linear}^{\mathbb{F}}\left(\mathcal{N}_P^k\right) \to 0$ as $k \to \infty$.*

Proof. In the previous theorem, take $t = \prod_{p \in P} P$ if P is finite and $t = \prod_{p \notin P} P$ if P is co-finite. □

The following corollary is a straightforward consequence of the theorem 4.2.23, and it is a generalization of [5, Theorem 1.2]. The proof is followed taking:

$$\mathcal{N}_t = \mathcal{N}_{\mathcal{A}_t} \bullet \mathcal{N}_{\mathcal{B}_t},$$

and for all $k \in \mathbb{N}$,

$$\mathcal{N}_t^k := \mathcal{N}_t^{\bullet k}\left[(t+2)^{2k}\right].$$

Then, we apply an argument as in the proof of the previous theorem.

Corollary 4.2.25. *There exists a infinite collection of sequences of networks*

$$\left\{\left(\mathcal{N}_t^k\right)_k : t \in \mathbb{N}, t \geq 2\right\}$$

in which each member of each sequence is asymptotically solvable but is not asymptotically linearly solvable and the linear capacity $\to 0$ as $k \to \infty$ in each sequence.

The network coding gain is equal to the coding capacity divided by the routing capacity. In [18, 33], there are two sequences of networks $\mathcal{N}_i(k)$ $(i = 1, 2)$ such that the coding gain $\to \infty$ as $k \to \infty$. The routing capacities of $\mathcal{N}_P^k$ and $\mathcal{N}_t^k$ are $\left(\frac{t+2}{2t+3}\right)^k$ and $\left(\frac{t^2+2t+4}{4t^2+12t+9}\right)^k$, respectively. Hence, any sequence of networks presented previously satisfies this property.

Corollary 4.2.26. *The network coding gain of the sequences $\left(\mathcal{N}_P^k\right)_k$ and $\left(\mathcal{N}_t^k\right)_k \to \infty$ as $k \to \infty$.*

4.3 Linear programming problems in secret sharing

Let Γ be an access structure on a set P with leader $p \notin P$. Given a secret sharing scheme

$$\Sigma = (S_x)_{x \in Q = P \cup p},$$

with access structure Γ, consider the random vector $(S_x)_{x \in Q}$,

$$h(X) := \mathrm{H}(S_X),$$

for every $X \subseteq Q$. Take

$$\alpha = \frac{1}{h(p)},$$

and the polymatroid (Q, f), with

$$f = \alpha h.$$

The function f can be seen as a vector $(f(X))_{X \subseteq Q}$ in $\mathbb{R}^{\mathcal{P}(Q)}$ that satisfies the following constraints:

(i) $f(p) = 1$,

(ii) $f(X \cup p) = f(X)$ for each $X \subseteq P$ with $X \in \Gamma$,

(iii) $f(X \cup p) = f(X) + 1$ for each $X \subseteq P$ with $X \notin \Gamma$,

(iv) information inequalities.

Therefore, f is a feasible solution of the following linear programming problem.

Problem 4.3.1. [17, 35] For any access structure Γ on a set P with leader $p \notin P$, $\kappa(\Gamma)$ is the optimal solution of the linear programming problem is to calculate $\min(v)$ such that

(i) $v \geq f(x)$ for each $x \in P$,

(ii) $f(X \cup p) = f(X)$ for each $X \subseteq P$ with $X \in \Gamma$,

(iii) $f(X \cup p) = f(X) + 1$ for each $X \subseteq P$ with $X \notin \Gamma$,

(iv) information inequalities.

We have

$$\kappa(\Gamma) \leq \sigma(\Gamma).$$

If we add linear rank inequalities in (iv), we have a linear programming problem whose optimal solution, denoted by $\kappa^*(\Gamma)$, holds

$$\kappa^*(\Gamma) \leq \lambda(\Gamma).$$

If we add characteristic-dependent linear rank inequalities, the Problem 4.3.1 gives a optimal solution that is a lower bound of $\lambda(\Gamma)$ of linear secret sharing schemes over specific fields; we denote this lower bounds by $\kappa^*_{\mathrm{char}(\mathbb{F})}(\Gamma)$, and the optimal information ratio of these schemes by $\lambda^*_{\mathrm{char}(\mathbb{F})}(\Gamma)$.

A known result about κ and matroids is as follows.

Theorem 4.3.2. *[26] Let Γ be an access structure. Then, Γ is a matroid port if and only if $\kappa(\Gamma) = 1$. Moreover, $\kappa(\Gamma) \geq \frac{3}{2}$ if Γ is not a matroid port.*

Example 4.3.3. In any port Γ of the Fano matroid, we have $\kappa(\Gamma) = \kappa^*_{\mathrm{char}(\mathbb{F})=2}(\Gamma) = \lambda^*_{\mathrm{char}(\mathbb{F})=2}(\Gamma) = 1$. They are ideal, see Example 1.4.1. Using the constraint (c) in Example 4.1.11 (this is obtained by the characteristic-dependent linear rank inequality over fields whose characteristic is different to 2 in Theorem 3.1.6), we directly get $\lambda^*_{\mathrm{char}(\mathbb{F})\neq 2}(\Gamma) = \kappa^*_{\mathrm{char}(\mathbb{F})\neq 2}(\Gamma) = \frac{4}{3}$; this value is achievable by a linear secret sharing scheme [23].

4.3.1 A class of ideal access structures

$$\begin{array}{c} \begin{array}{ccccccc} a_1 & \cdots & a_{t+1} & b_1 & \cdots & b_{t+1} & c \end{array} \\ \begin{pmatrix} 1 & \cdots & 0 & 0 & \cdots & 1 & 1 \\ 0 & \vdots & \vdots & 1 & \vdots & 1 & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \vdots & 0 & 1 & \vdots & 1 & \vdots \\ 0 & \cdots & 1 & 1 & \cdots & 0 & 1 \end{pmatrix} \end{array}$$

Figure 4.3.1: Family of matrices used to define access structures.

Let $t \in \mathbb{N}$, $t > 1$ and let $\mathbb{F}$ be a finite field. We use the port at c of the representable matroid obtained from the matrix in Figure 4.3.1; the set of participants is $P = \{a_1, \ldots, a_{t+1}, b_1, \ldots, b_{t+1}\}$, with dealer $p = c$.

When $\mathrm{char}(\mathbb{F})$ divides t, the following set is a subclass of the minimal authorized set of this matroid port:

$$\{a_1b_1, \ldots, a_{t+1}b_{t+1}, a_1 \cdots a_{t+1}, a_1b_2 \cdots b_{t+1}, b_1a_2b_3 \cdots b_{t+1}, \ldots, b_1 \cdots b_t a_{t+1}\}$$

and the following set is a subclass of the non-authorized set:

$$\{b_1a_2\cdots a_{t+1}, a_1b_2a_3\cdots a_{t+1}, \ldots, a_1\cdots a_tb_{t+1}\} \cup \{b_1\cdots b_{t+1}\}.$$

When $\mathrm{char}(\mathbb{F})$ does not divide t, the following set is a subclass of the minimal authorized set:

$$\{a_1b_1, \ldots, a_{t+1}b_{t+1}, a_1\cdots a_{t+1}, a_1b_2\cdots b_{t+1}, b_1a_2b_3\cdots b_{t+1}, \ldots, b_1\cdots b_ta_{t+1}\} \cup \{b_1\cdots b_{t+1}\}$$

and the following set is a subclass of the non-authorized set:

$$\{b_1a_2\cdots a_{t+1}, a_1b_2a_3\cdots a_{t+1}, \ldots, a_1\cdots a_tb_{t+1}\}.$$

So, we have defined two types of access structures using matroid ports. Let $\mathcal{F}_t$ be an access structure of the first type and let $\mathcal{N}_t$ be an access structure of the second type. We have the following proposition.

Proposition 4.3.4. *$\sigma(\mathcal{F}_t) = \lambda_{\mathrm{char}(\mathbb{F})|t}(\mathcal{F}_t) = \kappa(\mathcal{F}_t) = \kappa^*_{\mathrm{char}(\mathbb{F})|t}(\mathcal{F}_t) = 1$ and $\sigma(\mathcal{N}_t) = \lambda_{\mathrm{char}(\mathbb{F})\nmid t}(\mathcal{N}_t) = \kappa(\mathcal{N}_t) = \kappa^*_{\mathrm{char}(\mathbb{F})\nmid t}(\mathcal{N}_t) = 1$.*

4.3.1.1 Applications to secret sharing

We now show as some the characteristic-dependent linear rank inequalities presented in Chapter 6 are used to imply lower bounds on the linear information ratio over specific fields of the access structures previously defined.

Remark 4.3.5. Taking $n = 2t + 3$ in Example 3.2.1, we remark that the following inequality is a constraint that must be satisfied by linear secret sharing schemes over fields whose characteristic does not divide t

$$f(C) \leq \frac{1}{t+2}\sum_{i\in[t+1]} f(A_i) + f\left(C \mid A_{[t+1]}\right) + f\left(C; B_{[t+1]}\right)$$

$$\sum_{i\in[t+1]}\left[f\left(C; A_{[t+1]-i}\right) + f(C; B_i) + f(C \mid A_i, B_i) + f\left(C; A_{[t+1]-i}, B_i\right)\right];$$

and the following inequality is a constraint that must be satisfied by linear secret sharing schemes over fields whose characteristic divides t

$$f(C) \leq \frac{1}{t+3}\left[\sum_{i\in[t+1]} f(A_i) + f(B_1)\right] + f\left(C \mid B_{[t+1]}\right) + f\left(C \mid A_{[t+1]}\right)$$

$$+\sum_{i\in[t+1]}\left[f\left(C;A_{[t+1]-i}\right)+f\left(C;B_i\right)+f\left(C\mid A_i,B_i\right)+f\left(C;A_{[t+1]-i},B_i\right)+\mathrm{I}\left(C;B_{[t+1]-i}\right)\right].$$

Theorem 4.3.6. *Let $\mathcal{F}_t$ and $\mathcal{N}_t$ be the access structures previously defined. Then,*

$$\lambda_{\mathrm{char}(\mathbb{F})\nmid t}\left(\mathcal{F}_t\right)\geq\kappa^*_{\mathrm{char}(\mathbb{F})\nmid t}\left(\mathcal{F}_t\right)\geq\frac{t+2}{t+1}$$

and

$$\lambda_{\mathrm{char}(\mathbb{F})\mid t}\left(\mathcal{N}_t\right)\geq\kappa^*_{\mathrm{char}(\mathbb{F})\mid t}\left(\mathcal{N}_t\right)\geq\frac{t+3}{t+2}.$$

Proof. Taking $A_i=a_i$, $B_i=b_i$ and $C=c$ in the linear programming problem 4.3.1 with the constraints valid over fields whose characteristic does not divide t, The access structure $\mathcal{F}_t$ holds that $f\left(a_i\right)\leq v$, $f\left(a_i\right)\leq v$, $f\left(\emptyset\right)=0$, $f\left(c\right)=1$, $f\left(c\mid a_{[t+1]}\right)=f\left(c\mid a_i,b_i\right)=f\left(c;a_{[t+1]-i},b_i\right)=f\left(c;b_i\right)=f\left(c;a_{[t+1]-i}\right)=f\left(c\mid a_i,b_i\right)=f\left(c;a_{[t+1]-i},b_i\right)=0$. Thus, from the mentioned inequality, we get

$$1=f\left(c\right)\leq\frac{1}{t+2}\sum_{i\in[t+1]}f\left(a_i\right)\leq\frac{t+1}{t+2}v.$$

Therefore, $\kappa^*_{\mathrm{char}(\mathbb{F})\nmid t}\left(\mathcal{F}_t\right)\geq v\geq\frac{t+2}{t+1}$. In a similar way, the other inequalities are obtained. □

Remark 4.3.7. From [23], $\lambda_{\mathrm{char}(\mathbb{F})\nmid 2}\left(\mathcal{F}_2\right)=\kappa^*_{\mathrm{char}(\mathbb{F})\nmid 2}\left(\mathcal{F}_2\right)=\lambda_{\mathrm{char}(\mathbb{F})\mid 2}\left(\mathcal{N}_2\right)=\kappa^*_{\mathrm{char}(\mathbb{F})\mid 2}\left(\mathcal{N}_2\right)=\frac{4}{3}$. So, in previous theorem, the bound on $\mathcal{F}_2$ is tight but the bound on $\mathcal{N}_2$ is not tight.

5 Conclusions

$$\begin{pmatrix} B^{p_1}_{M(n_1,p_1)} & O & O \\ O & B^{p_1}_{M(n_1,p_1)} & O \\ O & O & B^{p_2}_{M(n_2,p_2)} \end{pmatrix}$$

Figure 5.0.1: Matrix such that $\text{rank}_{p_1} = 2M(n_1,p_1) + M(n_2,p_2) - 2$, $\text{rank}_{p_2} = 2M(n_1,p_1) + M(n_2,p_2) - 1$ and $\text{rank}_{p \neq p_1,p_2} = 2M(n_1,p_1) + M(n_2,p_2)$.

In this dissertation we study two methods for producing characteristic-dependent linear rank inequalities and show some applications. We explicitly calculate some of them. We remark that these inequalities are non-Shannon information inequalities. We make the following observations:

1. In the case of the first method, we derive some properties of the inequalities produced. In Example 2.2.1 are shown some inequalities but we remark that it did not show all inequalities that the method can produce because there are many suitable binary matrices that were not included; for example, in Figure 5.0.1 is shown a matrix that can be used to produce inequalities (the case $p_1 = 2$, $p_2 = 3$, $n_1 = 3$, $n_2 = 4$ produces the inequality in 21 variables that was shown in Chapter 2). We cannot ensure that the inequalities are independent of each other; this can be very complicated, in this direction, Corollary 2.2.2 showed a partial result. In future work, we can study its independence or dependence.

2. In the case of the second method, we think that the method can still reach a higher level of presentation for producing more inequalities. A clue can be found in [23]; studying other inequalities obtained by secret sharing schemes. We can also study the dependence or independence of these inequalities.

3. Future work can be found studying other properties of (k,n)-solvability problem of a closure operator. A clue can be found by studying that other propositions of [19, 20] are valid in this context.

4. The linear programming problems studied in this document are used to calculate capacities or radios of information from networks, closure operators or access structures. A computer implementation (adding the inequalities presented in this document) can be very useful; even with the networks and access structures that we have studied. The importance of such implementation in the classification of access structures on a small number of participants is remarkable in [3, 17].

5. It would be interesting to construct some linear secret sharing schemes that can achieve the bounds on the information ratios of the matroid ports in Theorem 4.3.6. The cases $\mathcal{F}_2$ and $\mathcal{N}_2$ were fully described in [23]. The technique presented to achieve these bounds cannot be extended in general to achieve other bounds in theorem 4.3.6 because these matroids do not have suitable hyperplane circuits; nevertheless, we think that the (λ, ω)-decomposition for secret sharing schemes in [47, 48] can be useful.

Bibliography

[1] R. Ahlswede, N. Cai, S.-Y. R. Li and R. W. Yeung. Network Information Flow. IEEE Transactions on Information Theory, 46(4): 1204-1216, 2000.

[2] N. Alon, E. Lubetzky, U. Stav, A. Weinstein, and A. Hassidim. Broadcasting with Side Information. IEEE Symposium on Foundations of Computer Science, pp. 823-832, 2008.

[3] M. Bamiloshin, A. Ben-Efraim, O. Farràs and C. Padró. Common Information, Matroid Representation, and Secret Sharing for Matroid Ports, 2019.

[4] Z. Bar-Yossef, Y. Birk, T. S. Jayram & T. Kol. Index Coding with Side Information. IEEE Symposium on Foundations of Computer Science, pp. 197–206, 2006. Also in IEEE Transactions on Information Theory, 57(3): 1479-1494, 2011.

[5] A. Blasiak, R. Kleinberg and E. Lubetzky. Lexicographic Products and the Power of non-Linear Network Coding. IEEE Symposium on Foundations of Computer Science, pp. 609-618, 2011.

[6] E. F. Brickell and D. M. Davenport. On the Classification of Ideal Secret Sharing, J. of Cryptology, 4:123-134, 1991.

[7] S. Burris and H. P. Sankappanavar. A Course in Universal Algebra, Springer-Verlag, 1981.

[8] J. Cannons, R. Dougherty, C. Freiling and K. Zeger. Network Routing Capacity. IEEE Transactions on Information Theory, 52(3): 7877-7888, 2006.

[9] T. H. Chan. Balanced Information Inequalities. IEEE Transactions of Information Theory, 49(12): 3261-3267, 2003.

[10] N. Das and B. K. Rai. On the Dependence of Linear Coding Rates on the Characteristic of the Finite Field, 2017.

[11] R. Dougherty, C. Freiling and K. Zeger. Insufficiency of Linear Coding in Network Information Flow. IEEE Transactions on Information Theory, 51(8): 2745-2759, 2005.

[12] R. Dougherty, C. Freiling and K. Zeger. Networks, Matroids, and non-Shannon Information Inequalities. IEEE Transactions on Information Theory, 53(6): 1949-1969, 2007.

[13] R. Dougherty, C. Freiling and K. Zeger. Linear Rank Inequalities on Five or More Variables. ArXiv 0910.0284, 2010.

[14] R. Dougherty, C. Freiling and K. Zeger. Achievable Rate Regions for Network Coding. IEEE Transactions on Information Theory, 61(5): 2488–2509, 2015. Also in ArXiv 1311.4601, 2013.

[15] R. Dougherty and K. Zeger. Non-Reversibility and Equivalent Constructions of Multiple-Unicast Networks, IEEE Transactions on Information Theory, 52(11):5067-5077, 2006.

[16] R. Dougherty. Computations of Linear Rank Inequalities on Six Variables. IEEE International Symposium on Information Theory, pp. 2819–2823, Hawaii, 2014.

[17] O. Farràs, T. Kaced, S. Martín and C. Padró. Improving the Linear Programming Technique in the Search for Lower Bounds in Secret Sharing, 2018.

[18] E. F. Freiling. Characteristic Dependent Linear Rank Inequalities and Applications to Network Coding. Dissertation for the Doctoral Degree. University of California, San Diego, 2014.

[19] M. Gadouleau, Closure solvability for Network Coding and Secret Sharing, IEEE Trans. Inform. Theory, UK , 59(12): 7858-7869, 2013.

[20] M. Gadouleau. Entropy of Closure Operators and Network Coding Solvability. Entropy, 16(9): 5122-5143, 2014.

[21] A. Gomez, C. Mejia, and J. A. Montoya. Linear Network Coding and the Model Theory of Linear Rank Inequalities. IEEE International Symposium on Network Coding, pp. 1-6, Aalborg, Denmark, 2014.

[22] A. W. Ingleton. Representation of Matroids. Combinatorial Mathematics and its Applications, pp. 149-167, Oxford, 1969.

[23] A. Jafari and S. Khazaei. On Abelian Secret Sharing: duality and separation, Cryptology ePrint Archive: Report 2019/575, 2019.

[24] R. Kinser. New Inequalities for Subspace Arrangements. Journal Combinatorial Theory Serie A, 118(1): 152-161, 2011.

[25] B. Lindström. On The Algebraic Characteristic Set for a Class of Matroids. Transactions of the American Mathematical Society, 95(1): 147–151, 1985.

[26] J. Martí-Farre, C. Padró. On Secret Sharing Schemes, Matroids and Polymatroids. J. Math. Cryptol. 4: 95-120, 2010.

[27] S. Martín, C. Padró and A. Yang. Secret Sharing, Rank Inequalities, and Information Inequalities, 2015.

[28] F. Matúš. Matroid Representations by Partitions, Discrete Math., 203: 169-194, 1999.

[29] F. Matúš. Two Constructions on Limits of Entropy Functions. IEEE Transactions on Information Theory, 53(1): 320-330, 2007.

[30] C. Mejia. Linear Secret Sharing and the Automatic Search of Linear Rank Inequalities. Applied Mathematical Science, 107(9): 5305-5324, DOI: 10.12988/ams.2015.57478, 2015.

[31] C. Mejia. On the Theory of Linear Rank Inequalities. Dissertation for the Doctoral Degree, Universidad Nacional de Colombia, Bogotá, 2016.

[32] C. Mejia and J. A. Montoya. On the Information Rates of Homomorphic Secret Sharing Schemes, Journal of Information and Optimization Sciences, 39(7): 1463-1482, DOI: 10.1080/02522667.2017.1367513, 2018.

[33] C. Ngai and R. Yeung. Network Coding Gain of Combination Networks. IEEE Information Theory Workshop, pp. 283–287, 2004.

[34] J. G. Oxley. Matroid Theory. Oxford University Press, New York, 1992.

[35] C. Padró. Lecture Notes in Secret Sharing. Cryptology ePrint Archive: Report 674, 2012.

[36] V. B. Peña Macias. Conexiones entre Codificación en Red, Operadores de Clausura y Matroides de Secreto Compartido, Dissertation for the Master Degree, Universidad Nacional de Colombia, Bogotá, 2015.

[37] V. Peña-Macias and H. Sarria. Characteristic-Dependent Linear Rank Inequalities via Complementary Vector Spaces, Journal of Information and Optimization Sciences, DOI: 10.1080/02522667.2019.1668157, 2020.

[38] V. Peña-Macias and H. Sarria. How to Find New Characteristic-Dependent Linear Rank Inequalities using Binary Matrices as a Guide, arXiv:1905.00003, 2019.

[39] V. Peña-Macias and H. Sarria. Characteristic-Dependent Linear Rank Inequalities in 21 variables, Revista Academia Colombiana de Ciencias Exactas, Físicas y Naturales, 43(169): 765-770, 2019.

[40] V. Peña-Macias and H. Sarria. Linear Programming Problems in Network Coding and Closure Operators via Partitions, Revista Selecciones Matemáticas, Universidad Nacional de trujillo, 6(2): 269-274, 2019.

[41] V. Peña-Macias. How to Find New Characteristic-Dependent Linear Rank Inequalities using Secret Sharing, Pre-print, 2019.

[42] S. Riis and M. Gadouleau. Graph-Theoretical Constructions for Graph Entropy and Network Coding based Communications. IEEE Transactions on Information Theory, 57(10): 6703–6717, 2011.

[43] P. D. Seymour. On Secret-Sharing Matroids, Journal of Combinatorial Theory, Series B, 56: 69-73, 1992.

[44] A. Shamir. How to Share a Secret, Communications of the ACM, 22(11): 612-613, 1979.

[45] A. Shen, D. Hammer, A. E. Romashchenko and N.K. Vereshchagin. Inequalities for Shannon Entropy and Kolmogorov Complexity. Journal of Computer and Systems Sciences, 60: 442-464, 2000.

[46] J. Simonis and A. Ashikhmin. Almost Affine Codes. Designs, Codes Cryptography, 14: 179-197, 1998.

[47] D. R. Stinson. Decomposition Constructions for Secret-Sharing Schemes. IEEE Transactions on Information Theory, 40(1): 118-125, 1994.

[48] M. Van-Dijk, W. A. Jackson, and K. M. Martin. A General Decomposition Construction for Incomplete Secret Sharing Schemes. Designs, Codes and Cryptography, 15(3): 301-321, 1998.

[49] R. Yeung. A First Course in Information Theory, Springer, Berlin, 2002.

[50] C. Yuan, H. Kan, W. Xin and I. Hideki. A Construction Method of Matroidal Networks, 2012.