KYBERNETIKA — VOLUME *59* (2023), NUMBER 2, PAGES 198–208

ACCESS STRUCTURES FOR FINDING CHARACTERISTIC-DEPENDENT LINEAR RANK INEQUALITIES

Victor Peña-Macias

Determining information ratios of access structures is an important problem in secret sharing. Information inequalities and linear rank inequalities play an important role for proving bounds on these ratios. Characteristic-dependent linear rank inequalities are rank inequalities which are true over vector spaces with specific field characteristic. In this paper, using ideas of secret sharing, we show a theorem that produces characteristic-dependent linear rank inequalities. These inequalities are then used for getting lower bounds on information ratios of some access structures in linear secret sharing.

Keywords: secret sharing, cryptography, access structures, matroids, complementary spaces, linear rank inequalities, entropy

Classification: 68P30, 94A15

1. INTRODUCTION

Secret sharing is a cryptographic protocol that consists of distributing a *secret* in several messages or *shares* within a set of participants, in such a way that if a *qualified subset* of participants shares their messages, these participants can discover the secret; but if a *non-qualified subset* of participants shares their messages, these participants cannot get any information about the secret [2, 5, 7]. A specific protocol with this property is called a *secret sharing scheme*, and the collection of subsets of participants with access to the secret is called an *access structure*. The efficiency of a scheme is measured by *information ratios* which relates the size of the secret and the size of the shares. In secret sharing, it is important to build efficient secret sharing schemes on an access structure. Therefore, determining the best information ratio, known as the *optimal information ratio*, is an important task.

A *linear rank inequality* is a linear inequality that is always satisfied by ranks (or dimensions) of subspaces of a vector space over any field. *Information inequalities* are a sub-class of linear rank inequalities [10]. A *characteristic-dependent linear rank inequality* is like a linear rank inequality but this is always satisfied by spaces over fields of certain characteristic and does not in general hold over other characteristics [3, 8, 9]. Information inequalities have been useful to estimate lower bounds on the optimal information ratio of access structures and linear rank inequalities have been useful to

DOI: 10.14736/kyb-2023-2-0198

estimate lower bounds on the optimal information ratio of access structures in *linear secret sharing*, i. e. when secret sharing schemes have a linear structure [4]. To the best of our knowledge, characteristic-dependent linear rank inequalities have not been used for determining bounds in linear secret sharing schemes over specific finite fields but due to the nature of distinguishing finite fields according to their characteristics, these inequalities can be potentially useful. One area where these inequalities have been useful for determining bounds is in *network coding* [1, 3, 8].

Contributions. In [5], Jafari and S. Khazaei developed a technique for proving lower bounds on access structures in linear secret sharing schemes on finite fields with a specific characteristic; the technique used access structures or *matroid ports* associated with the *Fano* and *non-Fano matroids*. We note that this technique can be improved for producing characteristic-dependent linear rank inequalities that also imply lower bounds on information ratios in linear secret sharing. In order to achieve this, we study some properties of vector spaces over finite fields related to complementary subspaces, we use known concepts of access structures such as qualified or non-qualified sets to facilitate the description of the properties. Then, using the vector deletion technique of Blasiak et al. in [1] which was improved in [8, 9], for each $n \geq 3$ we get a pair of inequalities that are true in any vector spaces over finite fields with specific field characteristic; these inequalities can be obtained as long as there exist binary matrices whose determinant is greater than one. We show some concrete inequalities using a well-known class of matrices and compute some lower bounds of optimal information ratios in linear secret sharing associated with access structures or ports of representable matroids over specific fields.

Organization of the work. In section 2 we study concepts and properties of information theory and vector spaces. We show the technique for producing characteristic-dependent linear rank inequalities which is summarized with a theorem. We then introduce concrete inequalities as a corollary. In subsection 2.1 we study some concepts of linear secret sharing and we compute lower bounds on information ratios of some matroid ports in linear secret sharing.

2. INEQUALITIES

Let $X_1, \ldots, X_m, X, Y$ be subspaces of a finite dimensional vector space V over a finite field $\mathbb{F}$. Let $\sum X_i$ be the span of X_i, $i \leq m$. We use the language of information theory, the dimension of a subspace is referred as the entropy, $\mathrm{H}(X_i : i \leq m) := \dim(\sum X_i)$. The *mutual information* of X and Y is given by $\mathrm{I}(X;Y) := \dim(X \cap Y)$. The *codimension of X in V* is $\mathrm{codim}_V(X) = \dim(V) - \dim(X)$ and we have the conditional information $\mathrm{H}(X \mid Y) := \mathrm{codim}_X(X \cap Y)$.

Let P be a proper subset of prime numbers and $I_1, \ldots, I_k \subseteq [m] = \{1, \ldots, m\}$. Let $\alpha_i \in \mathbb{R}$, for $i \leq k$. An inequality of the form $\sum \alpha_i \mathrm{H}(X_j : j \in I_i) \geq 0$ is called a *characteristic-dependent linear rank inequality* if it holds for all vector spaces $X_1, \ldots, X_m$ over a finite field whose characteristic is in P, and does not in general hold over other characteristics. Besides, the inequality is called a *linear rank inequality* if it holds for all vector spaces. Examples of such inequalities can be found in [3, 6, 8, 9].

We say that $\{X_i\}$ is *qualified* with respect to C if $C \leq \sum X_i$ and *non-qualified* with respect to C if $C \cap \sum X_i = O$. Secondly, we say that $\{X_i\}$ is *minimal qualified*

with respect to C (for short, minimal qualified) if $\{X_i\}$ is qualified and $\{X_i\}_{i\neq j}$ is non-qualified with respect to C, for each j; if we additionally have that $\{X_i : i \neq j\} \cup \{C\}$ is minimal qualified with respect to X_j for $j \leq m$, then $(X_1, \ldots, X_m, C)$ is said to be a *tuple of complementary vector spaces*.

A *complement* to a subspace of a vector space is another subspace which forms a direct sum; such spaces are *mutually complementary*. Therefore, a tuple of complementary vector spaces is a tuple of $m+1$ subspaces such that any m of them are mutually complementary and their span contains the missing subspace. Moreover, each non-zero vector of any of these subspaces can be uniquely written as a sum of non-zero vectors of the other subspaces; this implies that the subspaces have the same dimension.

Lemma 2.1. Let X_1, ..., X_m and C be subspaces of a finite dimensional vector space V such that $\{X_i\}$ is minimal qualified with respect to C. Then, there exist subspaces $\bar{X}_i \leq X_i$ for $i \leq m$ with dimension $\mathrm{H}(C)$ such that $\left(\bar{X}_1, \ldots, \bar{X}_m, C\right)$ is a tuple of complementary vector spaces and $\{X_i\}_{i\neq j}$ is non-qualified with respect to $\bar{X}_j$ for $j \leq m$.

P r o o f. In case C or some X_i are equal to $\{0\}$, we take $\bar{X}_i = \{0\}$ for all i. Otherwise, we assume that all subspaces are different from zero space. Let (e_i) be a basis of C. Using that $\{X_i\}$ is qualified, we obtain that each e_i can be written as $\sum_j e_i^j$ with $e_i^j \in X_i$. Define $\bar{X}_i = \left\langle e_i^j : j \right\rangle$; we ensure $\left(\bar{X}_1, \ldots, \bar{X}_m, C\right)$ is the desired tuple. Take $x = i\sum_i \alpha_i e_k^i \in \bar{X}_k \cap \sum_{i\neq k} X_i$ and define $c = i\alpha_i e_i \in C$ for getting $c = \sum_i \alpha_i \sum_j e_i^j = \sum_i \alpha_i e_k^i + \sum_j \sum_{i\neq k} \alpha_i e_i^j = x + \sum_j \sum_{i\neq k} \alpha_i e_i^j$. We have $c \in \sum_{i\neq k} X_i$ while $\{X_i\}_{i\neq k}$ is non-qualified, so $\alpha_i = 0$ for each i, in other words $x = 0$. Hence, $\{\bar{X}_i\}_{i\neq k}$ is non-qualified with respect to $\bar{X}_k$ for $k \leq m$. This also proves that $\bar{X}_i$ $i \leq n$ are minimal qualified with respect to C. On the other hand, fixed j, by definition of the subspaces $\bar{X}_i$ $i \leq n$, we have $\bar{X}_1$, ..., $\bar{X}_{j-1}$, C, $\bar{X}_{j+1}$, ..., $\bar{X}_m$ are qualified with respect to $\bar{X}_j$ and they are minimal qualified because otherwise we can get a subcollection of the subspaces $\bar{X}_i$ $i \leq n$, $i \neq j$, that would not be non-qualified with respect to C. The proof is completed. □

Let $n \geq 3$, we always consider a family $\mathscr{B} = \{b_1, \ldots, b_n\}$ of non-empty subsets of $[n]$. From this family, we can obtain a $n \times n$ binary matrix $B = (b_{ij})$ where $b_{ij} = \begin{cases} 1 & \text{if } i \in b_j \\ 0 & \text{other case} \end{cases}$. The following statement is a consequence of previous lemma.

Lemma 2.2. Let A_i for $i \leq n$, B_b for $b \in \mathscr{B}$ and C be subspaces of V such that $\{A_i : i \leq n\}$ and $\left\{\sum_{i\notin b} A_i, B_b\right\}$ for $b \in \mathscr{B}$ are minimal qualified with respect to C. Then, there exist subspaces with dimension $\mathrm{H}(C)$, $\bar{A}_i \leq A_i$ for $i \leq n$, $A^b \leq \sum_{i\notin b} A_i$ and $\bar{B}_b \leq B_b$ for $b \in \mathscr{B}$ such that $\left(\bar{A}_1, \cdots, \bar{A}_n, C\right)$ and $\left(A^b, \bar{B}_b, C\right)$ are tuples of complementary spaces.

Consider the subspaces whose existence was proved in previous lemma; they are not necessarily uniquely determined but we fix them. We can define the linear mapping $\varphi_B : C \to \bigoplus_{b\in\mathscr{B}} \frac{\sum_{i\notin b} \bar{A}_i}{A^b \cap \sum_{i\notin b} \bar{A}_i}$ given by $\varphi_B(c) := \sum_{b\in\mathscr{B}} \left[\sum_{i\notin b} a_i\right]_{A^b \cap \sum_{i\notin b} \bar{A}_i}$, where $c = \sum_i a_i$, $a_i \in \bar{A}_i$.

Lemma 2.3. Let A_i for $i \leq n$, B_b for $b \in \mathscr{B}$ and C be subspaces of V such that $\{A_i\}$ and $\left\{A_i \sum_{i \notin b}, B_b\right\}$ for $b \in \mathscr{B}$ are minimal qualified. Then

$$[n+1]\,\mathrm{H}(C) \leq \sum_{b \in \mathscr{B}} \mathrm{H}(A_i : i \notin b) + \mathrm{H}(\ker(\varphi_B)).$$

Proof.
From mapping φ_B, $\mathrm{H}(C) - \mathrm{H}(\ker(\varphi_B)) \leq \sum_{b \in \mathscr{B}} \left(\mathrm{H}\left(\bar{A}_i : i \notin b\right) - \mathrm{I}\left(A^b; \bar{A}_i : i \notin b\right)\right)$. Using $\mathrm{H}\left(A^b\right) = \mathrm{H}(C)$ and $A^b, \bar{A}_i \leq \sum_{i \notin b} A_i$, we obtain the inequality as follows

$$\begin{aligned}
\mathrm{H}(C) - \mathrm{H}(\ker(\varphi_B)) + n\mathrm{H}(C) &\leq \mathrm{H}(C) - \mathrm{H}(\ker\varphi_B) + \sum_{b \in \mathscr{B}} \mathrm{H}\left(A^b\right) \\
&\leq \left[\mathrm{H}\left(\bar{A}_i : i \notin b\right) + \mathrm{H}\left(A^b\right) - \mathrm{I}\left(A^b; \bar{A}_i : i \notin b\right)\right] \\
&= \sum_{b \in \mathscr{B}} \mathrm{H}\left(A^b, \bar{A}_i : i \notin b\right) \\
&\leq \sum_{b \in \mathscr{B}} \mathrm{H}(A_i : i \notin b).
\end{aligned}$$

□

Proposition 2.4. Let A_i for $i \leq n$, B_b for $b \in \mathscr{B}$ and C be subspaces of V over a finite field $\mathbb{F}$ whose characteristic does not divide $t = \det B$ such that $\{A_i\}$ and $\left\{\sum_{i \notin b} A_i, B_b\right\}$ for $b \in \mathscr{B}$ are minimal qualified; $\{B_b : b \in \mathscr{B}\}$ and $\left\{\sum_{i \in b} A_i, B_b\right\}$ for $b \in \mathscr{B}$ are non-qualified. Then $\ker(\varphi_B) = \{0\}$.

Proof. Let $c = \sum_i a_i \in C$, $a_i \in \bar{A}_i$ such that $\varphi_B(c) = 0$, we have to show $c = 0$. For $b \in \mathscr{B}$, we obtain $\sum_{i \notin b} a_i \in A^b$. From Lemma 2.2, there exists (unique) $b_b \in \bar{B}_b \leq B_b$ such that $\sum_{i \notin b} a_i + b_b \in C$. Hence, $\sum_{i \in b} a_i - b_b = c - \left(\sum_{i \notin b} a_i + b_b\right) \in C \cap \left(\sum_{i \in b} A_i + B_b\right)$. Observing that $\left\{\sum_{i \in b} A_i, B_b\right\}$ is non-qualified, we have $\sum_{i \in b} a_i = b_b$ and this holds for any $b \in \mathscr{B}$. We then obtain the matrix equation $B(a_i)_{i \leq n} = (b_b)_{b \in \mathscr{B}}$. Since the characteristic of $\mathbb{F}$ does not divide $t = \det B$, the matrix B is non-singular. Therefore, each a_i can be written as a linear combination of b_b, $b \in \mathscr{B}$, which implies that $c \in \sum_{b \in \mathscr{B}} B_b$, but $\{B_b : b \in \mathscr{B}\}$ is non-qualified, we get $c = 0$. □

Corollary 2.5. Let A_i for $i \leq n$, B_b for $b \in \mathscr{B}$ and C be subspaces of V over a finite field $\mathbb{F}$ such that $\{A_i\}$ and $\left\{\sum_{i \notin b} A_i, B_b\right\}$ for $b \in \mathscr{B}$ are minimal qualified; $\left\{\sum_{i \in b} A_i, B_b\right\}$ for $b \in \mathscr{B}$ is non-qualified. Then, for $b \in \mathscr{B}$ the mapping $\phi_B^b : \ker(\varphi_B) \to B_b$ given by $\phi_B^b(c) := b_b$ is an one-to-one linear function. Also, if the bth column of B is a linear combination of the columns of the submatrix B_X, $X \subseteq \mathscr{B}$. Then, $\phi_B^b(\ker(\varphi_B)) \subseteq \sum_{x \in X} B_x$.

There is a correspondence one-to-one between the families $\mathscr{B}$ with size n and the set of $n \times n$ binary matrices. Permutations of the columns of a matrix are equivalent to writing the members of $\mathscr{B}$ in a different order; the determinant of B can take other sign

or not. Depending on the finite field where the entries of B are defined, the matrix can be singular or not. We take advantage of these properties in order to use the previous propositions for producing inequalities. For any spaces, we find subspaces that satisfy those properties; we use the deletion technique of [1] which consists of finding convenient complementary spaces. It should be noted that these subspaces are not unique but we fix them. We summarize in the following theorem.

Theorem 2.6. For any $n \times n$ binary matrix B such that $\det B = t > 1$. Let A_i for $i \leq n$, B_b for $b \in \mathscr{B}$ and C be subspaces of V over a finite field $\mathbb{F}$. The following inequalities are characteristic-dependent linear rank inequalities:

— If the characteristic of $\mathbb{F}$ does not divide t, then

$$\mathrm{H}(C) \leq \frac{1}{n+1}\sum_{b\in\mathscr{B}}\mathrm{H}(A_i : i \notin b) + \mathrm{H}(C \mid A_i : i \leq n) + \sum_{b\in\mathscr{B}}\mathrm{H}_{b\in\mathscr{B}}(C \mid A_i, B_b : i \notin b)$$

$$+\sum_i \mathrm{I}(C; A_j : j \neq i) + \sum_{b\in\mathscr{B}}\mathrm{I}(C; B_b) + \sum_{b\in\mathscr{B}}\mathrm{I}(C; A_i, B_b : i \in b) + \mathrm{I}(C; B_b : b \in \mathscr{B}).$$

— If the characteristic of $\mathbb{F}$ divides t, then for $d \in \mathscr{B}$

$$\mathrm{H}(C) \leq \frac{1}{n+2}\left(\sum_{b\in\mathscr{B}}\mathrm{H}(A_i : i \notin b) + \mathrm{H}(B_d)\right) + \mathrm{H}(C \mid A_i : i \leq n)$$

$$+\mathrm{H}(C \mid B_b : b \in \mathscr{B}) + \sum_{b\in\mathscr{B}}\mathrm{H}(C \mid A_i, B_b : i \notin b) + \sum_i \mathrm{I}(C; A_j : j \neq i)$$

$$+\sum_{b\in\mathscr{B}}\mathrm{I}(C; B_b) + \sum_{b\in\mathscr{B}}\mathrm{I}(C; A_i, B_b : i \in b) + \sum_{b\in\mathscr{B}}\mathrm{I}(C; B_c : c \in \mathscr{B} - b)$$

The inequalities do not in general hold over fields whose characteristic is different to the mentioned. Counter examples would be in $V = \mathrm{GF}(p)^n$, take the vector spaces $A_i = \langle e_i \rangle$ for $i \leq n$ (vector with i-th component equal to 1 and the others 0), $B_b = \langle b_b \rangle$ for $b \in \mathscr{B}$ (the b-column of B) and $C = \langle \sum e_i \rangle$ (vector with 1 in all components). Then, when p divides t, the first inequality does not hold; and when p does not divide t, the second inequality does not hold.

P r o o f . Let $\mathbb{F}$ be a finite field whose characteristic does not divide t. For proving the first inequality we need to get subspaces of A_i for $i \leq n$, B_b for $b \in \mathscr{B}$, and C that satisfy hypotheses of Proposition 2.4. Let $C_0 := C \cap \sum_i A_i \cap \bigcap_{b\in\mathscr{B}} \left(\sum_{i\notin b} A_i + B_b\right)$. We have

$$\mathrm{H}(C \mid C_0) \leq \mathrm{H}(C \mid A_i : i \leq n) + \sum_{b\in\mathscr{B}}\mathrm{H}(C \mid A_i, B_b : i \notin b).$$

Recursively for $i \leq n$, denote by C_i a subspace of C_{i-1} which is a complement to $\sum_{j\neq i} A_j$ of $C_{i-1} + \sum_{j\neq i} A_j$. We have $\mathrm{H}(C_{i-1} \mid C_i) \leq \mathrm{I}(C; A_j : j \neq i)$. Let $\bar{C}_0 := C_n$, we have $\mathrm{H}\left(C_0 \mid \bar{C}_0\right) \leq \sum_{\mathrm{I}}(C; A_j : j \neq i)$. Recursively for each b_i $i \leq n$, denote by $\bar{C}_i$ a subspace of $\bar{C}_{i-1}$ which is a complement to B_{b_i} of $\bar{C}_{i-1} + B_{b_i}$. We have $\mathrm{H}\left(\bar{C}_{i-1} \mid \bar{C}_i\right) \leq \mathrm{I}(C; B_{b_i})$.

We denote $\tilde{C}_0 := \bar{C}_n$, then $\mathrm{H}\left(\bar{C}_0 \mid \tilde{C}_0\right) \leq \sum_{b\in\mathscr{B}} \mathrm{I}\left(C; B_b\right)$. Again recursively for each b_i $i \leq n$, denote by $\tilde{C}_i$ a subspace of $\tilde{C}_{i-1}$ which is a complement to $\sum_{j\in b_i} A_j + B_{b_i}$ of $\tilde{C}_{i-1} + \sum_{j\in b_i} A_j + B_{b_i}$. We also have $\mathrm{H}\left(\tilde{C}_{i-1} \mid \tilde{C}_i\right) \leq \mathrm{I}\left(C; A_j, B_{b_i} : j \in b_i\right)$. Then

$$\mathrm{H}\left(\tilde{C}_0 \mid \tilde{C}_n\right) \leq \sum_{b\in\mathscr{B}} \mathrm{I}\left(C; A_i, B_b : j \in b\right).$$

Finally define by $\hat{C}$ a subspace of $\tilde{C}_n$ which is a complement to $\sum_{b\in\mathscr{B}} B_b$ of $\tilde{C}_n + \sum_{b\in\mathscr{B}} B_b$. We have $\mathrm{H}\left(\tilde{C}_n \mid \hat{C}\right) \leq \mathrm{I}\left(C; B_b : b \in \mathscr{B}\right)$. Hence,

$$\begin{aligned}\mathrm{H}\left(C \mid \hat{C}\right) &= \mathrm{H}\left(C \mid C_0\right) + \mathrm{H}\left(C_0 \mid \bar{C}_0\right) + \mathrm{H}\left(\bar{C}_0 \mid \tilde{C}_0\right) + \mathrm{H}\left(\tilde{C}_0 \mid \tilde{C}_n\right) + \mathrm{H}\left(\tilde{C}_n \mid \hat{C}\right)\\ &\leq \mathrm{H}\left(C \mid A_i : i \leq n\right) + \sum_{b\in\mathscr{B}} \mathrm{H}\left(C \mid A_i, B_b : i \notin b\right) + \sum_i \mathrm{I}\left(C; A_j : j \neq i\right)\\ &\quad + \sum_{b\in\mathscr{B}} \mathrm{I}\left(C; B_b\right) + \sum_{b\in\mathscr{B}} \mathrm{I}\left(C; A_i, B_b : i \in b\right) + \mathrm{I}\left(C; B_b : b \in \mathscr{B}\right).\end{aligned}$$

We have $\{A_i\}$ and $\left\{\sum_{i\notin b} A_i, B_b\right\}$ for $b \in \mathscr{B}$ are minimal qualified with respect to $\hat{C}$; $\{B_b : b \in \mathscr{B}\}$ and $\left\{\sum_{i\in b} A_i, B_b\right\}$ for $b \in \mathscr{B}$ are non-qualified. Applying Proposition 2.4, we have $\ker\left(\varphi_B\right) = \{0\}$. Therefore, from inequality in Lemma 2.3,

$$[n+1]\,\mathrm{H}\left(\hat{C}\right) \leq \sum_{b\in\mathscr{B}} \mathrm{H}\left(A_i : i \notin b\right).$$

Using the last two inequalities, we obtain the desired inequality:

$$\mathrm{H}\left(C\right) - \mathrm{H}\left(C \mid A_i : i \leq n\right) - \sum_{b\in\mathscr{B}} \mathrm{H}\left(C \mid A_i, B_b : i \notin b\right) - \sum_i \mathrm{I}\left(C; A_j : j \neq i\right) - \sum_{b\in\mathscr{B}} \mathrm{I}\left(C; B_b\right)$$

$$- \sum_{b\in\mathscr{B}} \mathrm{I}\left(C; A_i, B_b : i \in b\right) - \mathrm{I}\left(C; B_b : b \in \mathscr{B}\right) \leq \mathrm{H}\left(\hat{C}\right) \leq \frac{1}{n+1} \sum_{b\in\mathscr{B}} \mathrm{H}\left(A_i : i \notin b\right).$$

For proving the second inequality, let $\mathbb{F}$ be a finite field whose characteristic divides t. Let $C_0' := C \cap \sum_i A_i \cap \sum_{b\in\mathscr{B}} B_b \cap \bigcap_{b\in\mathscr{B}} \left(\sum_i \notin bA_i + B_b\right)$. We apply to C_0' the same argument applied to space C_0 in the proof of the first inequality, we therefore obtain a subspace $\hat{C}_0 := \tilde{C}_n'$ such that

$$\begin{aligned}\mathrm{H}\left(C \mid \hat{C}_0\right) &\leq \mathrm{H}\left(C \mid A_i : i \leq n\right) + \mathrm{H}\left(C \mid B_b : b \in \mathscr{B}\right) + \sum\nolimits_{b\in\mathscr{B}} \mathrm{H}\left(C \mid A_i, B_b : i \notin b\right)\\ &\quad + \sum_i \mathrm{I}\left(C; A_j : j \neq i\right) + \sum_{b\in\mathscr{B}} \mathrm{I}\left(C; B_b\right) + \sum_{b\in\mathscr{B}} \mathrm{I}\left(C; A_i, B_b : i \in b\right).\end{aligned}$$

Recursively, for $i \leq n$, we denote by $\hat{C}_i$, a subspace of $\hat{C}_{i-1}$ which is a complement to $\sum_{b\in\mathscr{B}-b_i} B_b$ of $\hat{C}_{i-1} + \sum_{b\in\mathscr{B}-b_i} B_b$; we have $\mathrm{H}\left(\hat{C}_{i-1} \mid \hat{C}_i\right) \leq \mathrm{I}\left(C; B_b : b \in \mathscr{B} - b_i\right)$. We define $\check{C} := \hat{C}_n$ and the following inequality holds

$$\mathrm{H}\left(C \mid \check{C}\right) = \mathrm{H}\left(C \mid \hat{C}_0\right) + \mathrm{H}\left(\hat{C}_0 \mid \check{C}\right)$$

$$\leq \mathrm{H}\left(C \mid A_i : i \leq n\right) + \mathrm{H}\left(C \mid B_b : b \in \mathscr{B}\right) + \sum_{b\in\mathscr{B}} \mathrm{H}\left(C \mid A_i, B_b : i \notin b\right)$$

$$+ \sum_{b\in\mathscr{B}} \mathrm{I}\left(C; B_b\right) + \sum_{i} \mathrm{I}\left(C; A_j : j \neq i\right) + \sum_{b\in\mathscr{B}} \mathrm{I}\left(C; A_i, B_b : i \in b\right) + \sum_{b\in\mathscr{B}} \mathrm{I}\left(C; B_c : c \in \mathscr{B} - b\right).$$

We have $\{A_i\}$, $\{B_b\}_{b\in\mathscr{B}}$ and $\left\{\sum_{i\notin b} A_i, B_b\right\}$ for $b \in \mathscr{B}$ are minimal qualified with respect to $\tilde{C}$; and $\{\sum VA_i, B_b\}$ for $b \in \mathscr{B}$ is non-qualified. Applying Lemma 2.3, we have

$$[n+1]\,\mathrm{H}\left(\check{C}\right) \leq \sum_{b\in\mathscr{B}} \mathrm{H}\left(A_i : i \notin b\right) + \mathrm{H}\left(\ker\left(\varphi_B\right)\right).$$

Furthermore, as B is singular over fields whose characteristic divides t, there exist $d \in \mathscr{B}$ and $X \subseteq \mathscr{B}$ such that the d-th column of B is a linear combination of the columns indexed by members of X. So, from Corollary 2.5, $\mathrm{H}\left(\ker\left(\varphi_B\right)\right) \leq \mathrm{I}\left(B_d; B_b : b \in X\right)$. Moreover, as $\{B_b\}_{b\in\mathscr{B}}$ is minimal qualified, from Lemma 2.1, we take a subspace $\bar{B}_d$ of B_d with dimension $\mathrm{H}\left(\check{C}\right)$ such that $\{B_b : b \in \mathscr{B} - d\}$ is non-qualified with respect to $\bar{B}_d$. We have

$$\mathrm{H}\left(\check{C}\right) + \mathrm{I}\left(B_d; B_b : b \in X\right) \leq \mathrm{H}\left(\bar{B}_d\right) + \mathrm{I}\left(B_d; B_b : b \in \mathscr{B} - d\right) \leq \mathrm{H}\left(B_d\right).$$

This implies $\mathrm{H}\left(\ker\left(\varphi_B\right)\right) \leq \mathrm{H}\left(B_d\right) - \mathrm{H}\left(\check{C}\right)$. Therefore,

$$[n+2]\,\mathrm{H}\left(\check{C}\right) \leq \sum_{b\in\mathscr{B}} \mathrm{H}\left(A_i : i \notin b\right) + \mathrm{H}\left(B_d\right).$$

We obtain the desired inequality:

$$\mathrm{H}\left(C\right) - \mathrm{H}\left(C \mid A_i : i \leq n\right) - \mathrm{H}\left(C \mid B_b : b \in \mathscr{B}\right) - \sum_{b\in\mathscr{B}} \mathrm{H}\left(C \mid A_i, B_b : i \notin b\right)$$

$$- \sum_{i} \mathrm{I}\left(C; A_j : j \neq i\right) - \sum_{b\in\mathscr{B}} \mathrm{I}\left(C; B_b\right) - \sum_{b\in\mathscr{B}} \mathrm{I}\left(C; A_i, B_b : i \in b\right)$$

$$- \sum_{b\in\mathscr{B}} \mathrm{I}\left(C; B_c : c \in \mathscr{B} - b\right) \leq \mathrm{H}\left(\check{C}\right) \leq \frac{1}{n+2}\left(\sum_{b\in\mathscr{B}} \mathrm{H}\left(A_i : i \notin b\right) + \mathrm{H}\left(B_d\right)\right).$$

□

This theorem produces characteristic-dependent linear rank inequalities as long as there are suitable binary matrices. We now produce some characteristic-dependent linear rank inequalities using a convenient class of matrices. Let $n \geq 3$, define the $n \times n$ binary matrix $B_n = (b_{ij})$ given by $b_{ij} = \begin{cases} 0 & \text{if } i = j \\ 1 & \text{other case} \end{cases}$. Then the determinant of B_n is $n-1$. We have the following consequence.

Corollary 2.7. Let A_i $i \leq n$, B_i $i \leq n$ and C be subspaces of V over a finite field $\mathbb{F}$. The following inequalities are characteristic-dependent linear rank inequalities:

— If the characteristic of $\mathbb{F}$ does not divide $n-1$, then

$$\mathrm{H}(C) \leq \frac{1}{n+1}\sum_i \mathrm{H}(A_i) + \mathrm{H}(C \mid A_i : i \leq n) + \sum_i \mathrm{H}(C \mid A_i, B_i)$$

$$+\sum_i \mathrm{I}(C; A_j : j \neq i) + \sum_i \mathrm{I}(C; B_i) + \sum_i \mathrm{I}(C; A_j, B_i : j \neq i) + \mathrm{I}(C; B_i : i \leq n)\,.$$

— If the characteristic of $\mathbb{F}$ divides $n-1$, then

$$\mathrm{H}(C) \leq \frac{1}{n+2}\left(\sum_i \mathrm{H}(A_i) + \mathrm{H}(B_1)\right) + \mathrm{H}(C \mid A_i : i \leq n)$$

$$+\mathrm{H}(C \mid B_i : i \leq n) + \sum_i \mathrm{I}(C; B_i) + \sum_i \mathrm{H}(C \mid A_i, B_i)$$

$$+\sum_i \mathrm{I}(C; A_j : j \neq i) + \sum_i \mathrm{I}(C; A_j, B_i : j \neq i) + \sum_i \mathrm{I}(C; B_j : j \neq i)\,.$$

Other matrices can still be studied for finding inequalities. Let $n \geq 7$ and t integer such that $2 \leq t \leq \left\lfloor \frac{n-1}{2} \right\rfloor - 1$ and $m = n - t - 2$. Let $b_i = \sum_{j \neq i} e_j$ and define the $m \times m$-matrix B^t_m with i-column b_i for $1 \leq i \leq t+1$ and e_i for $t+2 \leq i \leq m$. The determinant of B^t_m is $\pm t$. Moreover, the 10×10 matrix shown in [9] can be obtained from B^2_3 and B^3_4.

2.1. Inequalities and linear secret sharing

Secret Sharing is an important component in many kinds of cryptographic protocols [2, 4, 7]. In a *secret sharing scheme*, a *secret* 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. We are interested in secret sharing over linear structures; this area is known as linear secret sharing. So, we restrict the concepts of secret sharing to the linear case, but the general theory can be easily followed by replacing vector spaces with random variables.

An *access structure*, denoted by Γ on a set of participants P, is a monotone increasing family of subsets of P. A set of participants X is said to be *qualified* if $X \in \Gamma$ and *non-qualified* if $X \notin \Gamma$. A *minimal qualified set* is a qualified set such that any proper subset is non-qualified. Consider a special participant $c \notin P$ called dealer. A *linear secret sharing scheme* on P with access structure Γ is a tuple of subspaces $\Sigma := (A_x)_{x \in P \cup \{c\}}$ such that the following properties are satisfied $\mathrm{H}(A_c) > 0$; if X is qualified, then $\mathrm{H}(A_c \mid A_x : x \in X) = 0$; if X is non-qualified, then $\mathrm{I}(A_c; A_x : x \in X) = 0$. The subspace A_c is the *secret* and the *shares* received by the participants are given by the subspaces A_x, $x \in P$.

The *information ratio* $\sigma(\Sigma)$ of the linear secret sharing scheme Σ is given by $\sigma(\Sigma) = \max_{x \in P} \frac{\mathrm{H}(A_x)}{\mathrm{H}(A_c)}$. The *optimal information ratio* $\lambda(\Gamma)$ of an access structure Γ is the infimum of the information ratios of all linear secret sharing schemes for Γ. In case we

want to specify the characteristic of the field, the optimal information ratio is written with a subscript.

The following linear programming problems are useful for calculating bounds on information ratios [4].

Problem 2.8. For any access structure Γ on a set P with leader $c \notin P$, the optimal solution $\kappa(\Gamma)$ of the linear programming problem is to calculate $\min v$ such that

(i) $v \geq f(x)$ for each $x \in P$.

(ii) $f(X \cup c) = f(X)$ for each $X \subseteq P$ with $X \in \Gamma$.

(iii) $f(X \cup c) = f(X) + 1$ for each $X \subseteq P$ with $X \notin \Gamma$.

(iv) Linear rank inequalities.

Consider a linear secret sharing scheme Σ, with access structure Γ, then the mapping given by $h(X) := \frac{1}{\mathrm{H}(A_c)}\mathrm{H}(A_x : x \in X)$, for $X \subseteq P \cup \{c\}$, satisfies the conditions of problem. Therefore, h is a feasible solution and we have $\kappa(\Gamma) \leq \lambda(\Gamma)$. In case we add inequalities that are true over fields with characteristic p in constraint (iv), we obtain a linear programming problem whose optimal solution, denoted by $\kappa_p(\Gamma)$, holds $\kappa_p(\Gamma) \leq \lambda_p(\Gamma)$.

A linear secret sharing scheme 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*. Given a matroid $\mathcal{M}$ with ground set $P \cup \{c\}$ and rank function r. The *port* of $\mathcal{M}$ at c is the access structure on P whose qualified sets are the sets $X \subseteq P$ satisfying $r(X \cup c) = r(X)$. Every ideal access structure is a matroid port and $\kappa(\Gamma) = 1$; moreover, $\kappa(\Gamma) \geq \frac{3}{2}$ if Γ is not a matroid port [7].

Let p be a prime number and consider the previously defined matrix B_n or its family of subsets denoted by $\mathscr{B}_n$. Define a representable matroid associated to the vectors e_i for $i \leq n$, b_b for $b \in \mathscr{B}_n$ and $c = \sum e_i$ over a finite field with characteristic p and take the access structure Γ_p obtained from the port at c. For example, Γ_2 is a port of Fano matroid and Γ_q, $q \neq 2$, is a port of non-Fano matroid.

We then have a matroid port Γ_p with $2n$ participants labeled as follow x_i for $i \leq n$, x_b for $b \in \mathscr{B}_n$. We note that $\{x_i : i \leq n\}$ and $\{x_i : i \notin b\} \cup \{x_b\}$ for $b \in \mathscr{B}_n$ are minimal qualified; and $\{x_i : i \in b\} \cup \{x_b\}$ is non-qualified for $b \in \mathscr{B}_n$. When p divides $n-1$, we have that $\{x_b : b \in \mathscr{B}_n\}$ is non-qualified; whereas when p does not divide $n-1$, this set is minimal qualified.

It is clear that Γ_p is ideal over a finite field with characteristic p but we do not know anything about the linear information ratio over fields with characteristic other than p. Inequalities in Corollary 2.7 can be used as constraints in Problem 2.8 for getting lower bounds on these ratios; the first inequality implies a constraint that must be satisfied by linear secret sharing schemes over fields whose characteristic does not divide $n-1$ and the second inequality implies a constraint that must be satisfied by linear secret sharing schemes over fields whose characteristic divides $n-1$.

In effect, let Γ_p such that p divides $n-1$ and consider Problem 2.8 with the constraint over fields whose characteristic does not divide $n-1$ given by Corollary 2.7. We have

that $f(x) \leq v$ for any participant x and $f(c) = 1$. The values of f corresponding to conditional information or mutual information that appear in the constraint are equal to 0. Thus, the constraint directly implies $1 = f(c) \leq \frac{1}{n+1}\sum_x f(x) \leq \frac{n}{n+1}v$; in other words, $\kappa_q(\Gamma_p) \geq v \geq \frac{n+1}{n}$ where q does not divide $n-1$. In a similar way, using the other constraint with an access structures Γ_p such that p does not divide $n-1$, we obtain the lower bound $\frac{n+2}{n+1}$ on $\kappa_q(\Gamma_p)$ where q divides $n-1$. We summarize in the following proposition.

Corollary 2.9. Let $\mathbb{F}$ be a finite field with characteristic p and $n \geq 3$. We have:

- If p divides $n-1$, then the access structure Γ_p is ideal over $\mathbb{F}$ and $\lambda_q(\Gamma_p) \geq \frac{n+1}{n}$ for any finite field whose characteristic q does not divide $n-1$.
- If p does not divide $n-1$, then the access structure Γ_p is ideal over $\mathbb{F}$ and $\lambda_q(\Gamma_p) \geq \frac{n+2}{n+1}$ for any finite field whose characteristic q divides $n-1$.

ACKNOWLEDGEMENT

The author thanks the support provided by COLCIENCIAS in Conv. 727; Carles Padró for the stay in Barcelona where these ideas were conceived; and the referees for the valuable suggestions which helped to improve the paper.

(Received June 7, 2022)

REFERENCES

[1] A. Blasiak, R. Kleinberg, and E. Lubetzky: Lexicographic products and the power of non-linear network coding. Ib: IEEE Symposium on Foundations of Computer Science 2011, pp. 609–618. DOI:10.1109/FOCS.2011.39

[2] E. F. Brickell and D. M. Davenport: On the classification of ideal secret sharing. J. Cryptology (1991), 4, 123–134. DOI:10.1007/BF00196772

[3] R. Dougherty, C. Freiling, and K. Zeger: Achievable Rate regions for network coding. IEEE Trans. Inform. Theory *61* (2015), 5, 2488–2509. DOI:10.1109/TIT.2015.2403315

[4] O. Farràs, T. Kaced, S. Martín, and C. Padró: Improving the linear programming technique in the search for lower bounds in secret sharing. IEEE Transactions on Information Theory 66 (2020), 11, 7088-7100. DOI:10.1109/TIT.2020.3005706

[5] A. Jafari and S. Khazaei: On Abelian secret sharing: Duality and separation. IACR Cryptol. ePrint Archive (2019), 575.

[6] S. Martín, C. Padró, and A. Yang: Secret Sharing, Rank Inequalities, and Information Inequalities. IEEE Trans. Inform. Theory *2* (2016), 1, 599–609. DOI:10.1109/TIT.2015.2500232

[7] C. Padró: Lecture notes in secret sharing. Cryptology ePrint Archive: Report (2012), 674.

[8] V. Peña-Macias and H. Sarria: Characteristic-dependent linear rank inequalities via complementary vector spaces. J. Inform. Optim. Sci. *42* (2021), 2, 345–369. DOI:10.1080/02522667.2019.1668157

[9] V. Peña-Macias and H. Sarria: Characteristic-dependent linear rank inequalities in 21 variables. Rev. Acad. Colomb. Cienc. Ex. Fis. Nat. *43* (2019), 169, 76-5-770. DOI:10.18257/raccefyn.928

[10] A. Shen, D. Hammer, A. E. Romashchenko, and N. K. Vereshchagin: Inequalities for Shannon Entropy and Kolmogorov Complexity. J. Computer Systems Sci. *60* (2000), 442–464. DOI:10.1006/jcss.1999.1677

Victor Peña-Macias, Departamento de Ciencias Básicas, Universitaria Virtual Internacional, Bogotá. Colombia.

e-mail: vbpenam@uvirtual.edu.co