




A theorem about linear rank inequalities that depend on the characteristic of the finite field

Un teorema sobre desigualdades rango lineales que dependen de la característica del cuerpo finito

Victor Peña-Macias 

Received, Jan. 21, 2022

Accepted, Jul. 11, 2022



How to cite this article:

Peña-Macias V. A theorem about linear rank inequalities that depend on the characteristic of the finite field. *Selecciones Matemáticas*. 2022;9(1):150–160. <http://dx.doi.org/10.17268/sel.mat.2022.01.12>

Abstract

A linear rank inequality is a linear inequality that holds by dimensions of vector spaces over any finite field. A characteristic-dependent linear rank inequality is also a linear inequality that involves dimensions of vector spaces but this holds over finite fields of determined characteristics, and does not in general hold over other characteristics. In this paper, using as guide binary matrices whose ranks depend on the finite field where they are defined, we show a theorem which explicitly produces characteristic-dependent linear rank inequalities; this theorem generalizes results previously obtained in the literature.

Keywords . Mutually complementary vector spaces, Binary matrix, Finite field, Entropy, Linear rank inequality.

Resumen

Una desigualdad rango lineal es una desigualdad lineal que es válida para dimensiones de espacios vectoriales sobre un cuerpo finito. Una desigualdad rango lineal dependiente de la característica es también una desigualdad lineal para dimensiones de espacios vectoriales pero ésta es válida sobre cuerpos finitos de determinada característica, y no es válida en general sobre otras características. En este documento, usando como guía matrices binarias cuyos rangos dependen del cuerpo finito en donde están definidas, nosotros presentamos un teorema que produce explícitamente desigualdades rango lineales dependientes de la característica; éste teorema generaliza resultados obtenidos previamente en la literatura.

Palabras clave. Espacios vectoriales mutuamente complementarios, Matriz binaria, Cuerpo finito, Entropía, Desigualdad rango lineal.

1. Introduction. A linear rank inequality is a linear inequality that is always satisfied by dimensions (usually referred as ranks in information theory) of subspaces of a vector space over any field. Information inequalities are a sub-class of linear rank inequalities [10]. Examples of these inequalities have been presented in [3, 5, 6]. 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. In information theory, especially in linear network coding, all these inequalities are useful to calculate linear rates of communication networks [1, 2, 4, 9, 11]. Hence the importance of finding this type of inequalities. Characteristic-dependent linear rank inequalities have been presented by Blasiak, et al. [1]; Dougherty et al. [4]. In [7, 8], we show some inequalities using the ideas of Blasiak and applications to network coding that improve some existing results.

We remark that in [1] two characteristic-dependent linear rank inequalities are produced in 7 variables; the first inequality is valid over finite fields with characteristic two and the second inequality is valid over finite fields with characteristic different from two. In [7], two inequalities are produced in n variables, for each n of the form $2t + 3$, $t \geq 2$; the first inequality is valid over finite fields whose characteristic divides

*Facultad de Ciencias, Universidad Nacional de Colombia, Colombia. (vbpenam@unal.edu.co).

t and the second inequality is valid over finite fields whose characteristic does not divide t . Obtaining, for each finite or co-finite set of prime numbers, an inequality that is valid over finite fields whose characteristic is in this set. In [8], three inequalities in 21 variables are produced. The first inequality is valid on finite fields of characteristic two; the second inequality in characteristic three; and the third inequality in characteristics different from two and three. Inequalities presented in [1, 7, 8] use a different technique than the technique used in [4].

2. Contributions and organization of the work. In this paper, we continue studying the technique presented in [1, 7, 8]. We show a theorem that explicitly produces characteristic-dependent linear rank inequalities whenever there exists a $n \times m$ binary matrix whose rank is different over different field characteristic¹. The inequalities presented in [1, 7, 8] can be deduced as particular cases where the binary matrix is of a specific form. Therefore, the theorem summarizes the method for producing inequalities in [1, 7, 8]. As a corollary, for each $n \geq 7$, we write $2 \lfloor \frac{n-1}{2} \rfloor - 4$ characteristic-dependent linear rank inequalities in n variables for any $n \geq 7$. This paper is organized as follows. In the next section, we give some definitions, we show the main theorem and produce inequalities. The proof of the theorem is showed in appendix.

2.1. Inequalities . The concepts treated in this paper are basic concepts of linear algebra that use the language of information theory to facilitate their writing. Let A, A_1, \dots, A_n, B be vector subspaces of a finite dimensional vector space V over a finite field \mathbb{F} . Let $\sum A_i$ be the span of $A_i, i \in I := \{1, \dots, n\}$. The entropy of A_1, \dots, A_n is

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

For simplicity, we have relaxed the formal definition of entropy of random variables induced by vector spaces. We remark that there is no loss of generality since the entropy of these variables is a fixed positive multiple scalar of the dimension of span of the vector spaces involved. For more details, see [8, 10]. Other measures are given as follows. The mutual information of A and B is given by

$$I(A; B) := \dim(A \cap B).$$

If B is a subspace of a subspace A , the *codimension* of B in A is given by $\text{codim}_A(B) := \dim(A) - \dim(B)$. We have

$$H(A | B) := \text{codim}_A(A \cap B).$$

Let P be a proper subset of primes, and let S_1, \dots, S_k be subsets of $\{1, \dots, m\}$. Let $\alpha_i \in \mathbb{R}$ for $1 \leq i \leq k$. An inequality of the form $\sum_i \alpha_i H(A_j : j \in S_i) \geq 0$ is called a *characteristic-dependent linear rank inequality* if it holds for all vector spaces A_1, \dots, A_m over finite fields with characteristic in P , and does not in general hold over other characteristics.

A linear rank inequality is an inequality with the same form but this is true over any field characteristic [5]. Therefore, a characteristic-dependent linear rank inequality is like a linear rank inequality that is true over some fields.

Let $m \leq n$, for any $n \times m$ binary matrix B with entries in a finite field \mathbb{F} , we denote the i -th column of B as e_{S_i} where $S_i = \{j : b_{ji} = 1\}$, and define the sets:

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

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

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

The set $\{e_1, \dots, e_n\}$ is the canonical basis in \mathbb{F}^n . We also denote $e_i = e_{S_i}$ if $|S_i| = 1$. In this paper, we consider vector subspaces labeled by the canonical basis and the set $\mathcal{B}' = \{e_{S_{j_1}}, \dots, e_{S_{j_{|\mathcal{B}'|}}}\}$.

¹This paper is an improved version of our preprint arXiv:1905.00003 and these results are part of the author's doctoral thesis entitled "New Characteristic Dependent Linear Rank Inequalities".

The following interval notation is convenient:

$$[e_k, e_j] := \{e_i : k \leq i \leq j\},$$

$$[e_k, e_j) := \{e_i : k \leq i < j\},$$

$$[e_k] := [e_1, e_k] = \{e_i : i \leq k\}.$$

For any A_{e_1}, \dots, A_{e_n} and C we define:

$$\nabla(C) := H(C | A_{[e_n]}) + \sum_{e_i \in [e_n]} I(A_{[e_n]-e_i}; C).$$

For each $T \subseteq [e_n]$, it is straightforward to take some vectors e_{k_1}, \dots, e_{k_l} in T with $k_1 \leq k_2 \leq \dots \leq k_l$ such that the intervals $[e_{k_1}, e_{k_2}), [e_{k_2}, e_{k_3}), \dots, [e_{k_{l-1}}, e_{k_l}]$ are blocks, with maximum length, of a partition of T . We remark that this partition is unique. We define:

$$\nabla(A_e : e \in T) := I(A_{[e_1, e_{k_1}]}; A_{[e_{k_1}, e_{k_2}]}) + I(A_{[e_1, e_{k_2}]}; A_{[e_{k_2}, e_{k_3}]}) + \dots + I(A_{[e_1, e_{k_{l-1}}]}; A_{[e_{k_{l-1}}, e_{k_l}]})$$

The following theorem is the main theorem of this paper and gives a method for producing characteristic-dependent linear rank inequalities from binary matrices whose rank is different over different field characteristic. The demonstration is presented in appendix 4.

Theorem 2.1. *Let B be a $n \times m$ binary matrix over a finite field \mathbb{F} , $m \leq n$ and $t_s, \dots, t_1 \geq 2$, $m > m_s > \dots > m_1 \geq 1$ integers. We suppose that $\text{rank}(B) = m_k$ if $\text{char}(\mathbb{F})$ divides t_k , $k = 1, \dots, s$, and $\text{rank}(B) = m$ in other cases. Let $A_{e_1}, \dots, A_{e_n}, B_{e_{S_{j_1}}}, \dots, B_{e_{S_{j_{|B'|}}}}$ and C be vector subspaces of a finite dimensional vector space V over a finite field \mathbb{F} . Then*

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

$$\begin{aligned} & H(A_{e_j}, B_{e_{S_i}}, C : e_{S_i} \in \mathcal{B}', e_j \in \mathcal{B}'', C \in \mathcal{B}''') + (|\mathcal{B}''| |\mathcal{B}'| + |\mathcal{B}''|) H(C) \leq m_k I(A_{[e_n]}; C) \\ & + \sum_{e_{S_k} \in \mathcal{B}'} \left[H(B_{e_{S_k}} | A_{e_i}, C : i \notin S_k) + H(B_{e_{S_k}} | A_{e_i} : i \in S_k) \right] + (|\mathcal{B}'| + 1) \sum_{e_i \in \mathcal{B}''} H(A_{e_i}) \\ & + (|\mathcal{B}''| |\mathcal{B}'| + |\mathcal{B}'''| + |\mathcal{B}''| + |\mathcal{B}'|) \left[H(C | A_{[e_n]}) + \sum_{e_i \in [e_n]} I(A_{[e_n]-e_i}; C) \right] \\ & + \sum_{e_{S_k} \in \mathcal{B}'} [\nabla(A_{e_i} : i \in S_k, e_i \notin \mathcal{B}'') + \nabla(A_{e_i} : i \notin S_k, e_i \notin \mathcal{B}'')]. \end{aligned}$$

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

$$\begin{aligned} & H(C) \leq \frac{1}{m} H(A_{e_j}, B_{e_{S_i}}, C : e_{S_i} \in \mathcal{B}', e_j \in \mathcal{B}'', C \in \mathcal{B}''') + H(C | A_{[e_n]}) \\ & + \sum_{e_i \in [e_n]} I(A_{[e_n]-e_i}; C) + \sum_{e_{S_k} \in \mathcal{B}'} \left[H(C | A_{e_i}, B_{S_k} : i \notin S_k) + H(B_{e_{S_k}} | A_{e_i} : i \in S_k) \right] \\ & + \sum_{e_{S_k} \in \mathcal{B}'} [\nabla(A_{e_i} : i \notin S_k) + \nabla(A_{e_i} : i \in S_k)]. \end{aligned}$$

The inequalities (i) do not in general hold over vector spaces whose characteristic does not divide t and the inequality in item (ii) does not in general hold over vector spaces whose characteristic divides t . A counterexample would be in $V = \text{GF}(p)^n$, take the vector spaces $A_{e_i} = \langle e_i \rangle$, $i \in [n]$, $B_{e_{S_j}} = \langle e_{S_j} \rangle$, $e_{S_j} \in \mathcal{B}'$, and $C = \langle \sum e_i \rangle$ Then,

$$H(A_{e_i}) = H(B_{e_{S_j}}) = H(C) = I(A_{[e_n]}; C) = 1,$$

$$H(B_{e_{S_k}} | A_{e_i}, C : i \notin S_k) = H(B_{e_{S_k}} | A_{e_i} : i \in S_k) = H(C | A_{[e_n]}) = 0,$$

$$H(C | A_{e_i}, B_{S_k} : i \notin S_k) = I(A_{[e_n]-e_i}; C) = 0,$$

$$\nabla(A_{e_i} : i \in S_k, e_i \notin \mathcal{B}'') = \nabla(A_{e_i} : i \notin S_k, e_i \notin \mathcal{B}'') = 0,$$

$$H(A_{e_j}, B_{e_{S_i}}, C : e_{S_i} \in \mathcal{B}', e_j \in \mathcal{B}'', C \in \mathcal{B}''') = \begin{cases} m_k, & \text{if } \text{char}(\mathbb{F}) \mid t_k \\ m, & \text{if } \text{char}(\mathbb{F}) \nmid t. \end{cases}$$

Therefore, when p does not divide t , the inequalities (i) do not hold; and when p divides t , the inequality (ii) does not hold.

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

Figure 2.1: Matrix $B_{M(n,t)}^t$ whose rank is $M(n,t)$ or $M(n,t) - 1$ according to the field characteristic.

Below is shown a class of $\lfloor \frac{n-1}{2} \rfloor - 2$ inequalities that are true over finite fields with characteristic in a finite set of primes; and another class of $\lfloor \frac{n-1}{2} \rfloor - 2$ inequalities that are true over finite fields with characteristic in a co-finite sets of primes.

Corollary 2.1. *Let $n \geq 7$, t integer such that $2 \leq t \leq \lfloor \frac{n-1}{2} \rfloor - 1$ and $M(n,t) = n - t - 2$. For any $A_1, A_2, \dots, A_{M(n,t)}, B_1, B_2, \dots, B_{t+1}$ and C subspaces of a finite dimensional vector space V over a finite field \mathbb{F} , we have:*

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

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

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

$$\begin{aligned}
 &+ [(t + 2) (M(n, t) - t) - 1] \left(H(C | A_{[M(n,t)]}) + \sum_{i=1}^{M(n,t)} I(A_{[M(n,t)]-i}; C) \right) \\
 &+ \sum_{i=1}^{t+1} (H(B_i | A_i, C) + H(B_i | A_{[M(n,t)]-i}) + I(A_{[i]; A_{[i+1,t+1]}}) + I(A_{[i-1]; A_i)).
 \end{aligned}$$

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

$$\begin{aligned}
 H(C) &\leq \frac{1}{M(n, t)} H(B_{[t+1]}, A_{[t+2, M(n,t)]}) + H(C | A_{[M(n,t)]}) + \sum_{i=1}^{M(n,t)} I(A_{[M(n,t)]-i}; C) \\
 &+ \sum_{i=1}^{t+1} (H(C | A_i, B_i) + H(B_i | A_{[M(n,t)]-i}) + I(A_{[i]; A_{[i+1, M(n,t)]}}) + I(A_{[i-1]; A_i)).
 \end{aligned}$$

Proof: Fixed n and t . In Theorem 2.1, we take the binary square matrix $B_{M(n,t)}^t$ as described in Figure 2.1. The rank of $B_{M(n,t)}^t$ is $M(n, t)$ when $\text{char}(\mathbb{F})$ does not divide t and is $M(n, t) - 1$ in other case. We have $|B'_{B_{M(n,t)}^t}| = t + 1$, $|B''_{B_{M(n,t)}^t}| = M(n, t) - t - 1$ and $|B'''_{B_{M(n,t)}^t}| = 0$. We denote $B_i := B_{e_{[M(n,t)]-i}}$, $A_i := A_{e_i}$ and have

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

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

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

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

With this in mind, the inequalities are obtained. We remark the use of interval notation as used in previous theorem. □

Remark 2.1. If we take $n = 2t + 3$, $M(n, t) = t + 1$, we obtain inequalities in [7]. Also, $t = 2$ implies inequalities in [1].

3. Conclusions. In this paper, we have presented a theorem that works as a method for producing characteristic-dependent linear rank inequalities whenever there exists a binary matrix whose rank is different according to the characteristic of the finite field where its entries are defined. In Corollary 2.1 are shown some inequalities obtained but we remark that this corollary does not show all inequalities that the method can produce because there are many suitable binary matrices that were not included. For example, in Figure 3.1 is shown a matrix that can be used for producing inequalities; case $p_1 = 2, p_2 = 3, n_1 = 3, n_2 = 4$ produces the characteristic-dependent linear rank inequalities in [8].

$$\begin{pmatrix} B_{M(n_1, p_1)}^{p_1} & O & O \\ O & B_{M(n_1, p_1)}^{p_1} & O \\ O & O & B_{M(n_2, p_2)}^{p_2} \end{pmatrix}$$

Figure 3.1: Binary 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 $\text{rank}_{p \neq p_1, p_2} = 2M(n_1, p_1) + M(n_2, p_2)$.

4. Acknowledgements. The author thanks to COLCIENCIAS for the support provided in Conv. 727, Prof. Humberto Sarria and the Universidad Nacional de Colombia.

ORCID and License

Victor Peña-Macias <https://orcid.org/0000-0002-4020-015X>

This work is licensed under the [Creative Commons - Attribution 4.0 International \(CC BY 4.0\)](https://creativecommons.org/licenses/by/4.0/)

References

- [1] Blasiak A, Kleinberg R, Lubetzky E. Lexicographic Products and the Power of non-Linear Network Coding, IEEE Symposium on Foundations of Computer Science. 2011; 609-618.
- [2] Dougherty R, Freiling C, Zeger K. Insufficiency of Linear Coding in Network Information Flow, IEEE Transactions on Information Theory, 2005; 51(8):2745-2759.
- [3] Dougherty R, Freiling C, Zeger K. Linear Rank Inequalities on Five or More Variables, ArXiv 0910.0284; 2010.
- [4] Dougherty R, Freiling C, Zeger K. Achievable Rate Regions for Network Coding, IEEE Transactions on Information Theory. 2015; 61(5):2488-2509.
- [5] Ingleton AW. Representation of Matroids. Combinatorial Mathematics and its Applications, Oxford. 1969; 149-167.
- [6] Kinsler R. New Inequalities for Subspace Arrangements, Journal Combinatorial Theory Serie A. 2011; 118(1):152-161.
- [7] Peña-Macias V, Sarria H. Characteristic-Dependent Linear Rank Inequalities via Complementary Vector Spaces, J. of Information and Optimization Sciences. 2021; 42(2):345-369. DOI: 10.1080/02522667.2019.1668157
- [8] Peña-Macias V, Sarria H. Characteristic-Dependent Linear Rank Inequalities in 21 variables, Revista Academia Colombiana de Ciencias Exactas, Físicas y Naturales. 2019; 43(169):765-770. <https://doi.org/10.18257/raccefyn.928>
- [9] Peña-Macias V, Sarria H. Linear Programming Problems in Network Coding and Closure Operators via Partitions, Revista Selecciones Matemáticas. 2019; 6(2):269-274. <http://dx.doi.org/10.17268/sel.mat.2019.02.12>
- [10] Shen A, Hammer D, Romashchenko AE, Vereshchagin NK. Inequalities for Shannon Entropy and Kolmogorov Complexity, Journal of Computer and Systems Sciences. 2000; 60:442-464.
- [11] Yeung R. A First Course in Information Theory, Springer, Berlin; 2002.

Appendix A. Proof of main theorem.

We use concepts of complementary vector spaces. Vector spaces A_{e_1}, \dots, A_{e_n} are mutually complementary spaces, if the span is a direct sum. In other words, every vector of span has a unique representation as a sum of elements of A_{e_1}, \dots, A_{e_n} ; we denote this span by $A_{e_1} \oplus \dots \oplus A_{e_n}$. In this case, π_I denotes the I -projection function $\bigoplus_{i \in I} A_{e_i} \rightarrow \bigoplus_{i \in I} A_{e_i}$ given by $x = \sum_{i \in I} x_i \mapsto \sum_{i \in I} x_i$. If there exists a vector subspace C of V such that $A_{e_1} \oplus \dots \oplus A_{e_{i-1}} \oplus C \oplus A_{e_{i+1}} \oplus \dots \oplus A_{e_n} \leq V$ for all i , then we say that $(A_{e_1}, \dots, A_{e_n}, C)$ is a tuple of complementary vector spaces.

Before showing the proof of the main theorem or Theorem 2.1, we develop three propositions and four lemmas. This makes the proof simpler.

Proposition A.1. Let $B = (e_{S_i})$ be a $n \times m$ binary matrix over a finite field \mathbb{F} , $m \leq n$ and $t_k \geq 2$, for $i = 1, \dots, s$, $m > m_s > \dots > m_1 \geq 1$ integers. We suppose that $\text{rank}(B) = m_k$ if $\text{char}(\mathbb{F})$ divides t_k , and $\text{rank}(B) = m$ in other cases. Then, any tuple of complementary vector spaces $(A_{e_1}, \dots, A_{e_n}, C)$ holds

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

Proof: In case $\text{char}(\mathbb{F})$ does not divide t , $\sum_{i \in [m]} \pi_{S_i}(C)$ is a direct sum by Corollary 9 in [8]. Then, we have

$$H(\pi_{S_i}(C) : i \in [m]) = \sum_{i \in [m]} H(\pi_{S_i}(C)) = m H(C) \quad [\text{from Proposition 6 in [8]}].$$

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

$$H(\pi_{S_i}(C) : i \in [m]) = H(\pi_{S_i}(C) : i \in I)$$

$$\begin{aligned}
 &= \sum_{i \in I} H(\pi_{S_i}(C)) \quad [\text{from Corollary 9 in [8]}] \\
 &= m_k H(C) \quad [\text{from Proposition 6 in [8]}].
 \end{aligned}$$

□

In previous proposition, the dependence relations of B , fixed a characteristic field, can be expressed using projections of a suitable space C . The following two propositions get inequalities that depend on the characteristic of \mathbb{F} , and the involved spaces have some dependency relationships expressed by B .

Proposition A.2. For each t_k , let \mathbb{F} be a finite field such that $\text{char}(\mathbb{F})$ divides t_k . For any vector subspaces $A_{e_1}, \dots, A_{e_n}, B_{e_{S_{j_1}}}, \dots, B_{e_{S_{j_{|B'|}}}}$ and C of a finite dimensional vector space V over \mathbb{F} , such

that $(A_{e_1}, \dots, A_{e_n}, C)$ is a tuple of complementary vector spaces and

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

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

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

We have

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

Proof: See Lemma 5 in [7] and Proposition 11 in [8].

□

Proposition A.3. Let \mathbb{F} be a finite field such that $\text{char}(\mathbb{F})$ does not divide $t = \prod_i t_i$. For any vector subspaces $A_{e_1}, \dots, A_{e_n}, B_{e_{S_{j_1}}}, \dots, B_{e_{S_{j_{|B'|}}}}$ and C of a finite dimensional vector space V over \mathbb{F} , such

that $(A_{e_1}, \dots, A_{e_n}, C)$ is a tuple of complementary vector subspaces and

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

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

We have

$$mH(C) \leq H(A_{e_i}, B_{e_{S_j}}, C : e_{S_j} \in B', e_i \in B'', C \in B''').$$

Proof: See Lemma 6 in [7] and Proposition 11 in [8].

□

Lemma A.1. For any A_{e_1}, \dots, A_{e_n} and C vector subspaces of a finite dimensional vector space V , there exists a tuple of complementary vector spaces $(A'_{e_1}, \dots, A'_{e_n}, \bar{C})$ such that $A'_{e_i} \leq A_{e_i}, \bar{C} \leq C, \bigoplus A'_{e_i} = \sum A_{e_i}$,

$$H(A_{e_i} | A'_{e_i}) = I(A_{[e_{i-1}]}; A_{e_i}), \quad i = 1, \dots, n, \tag{A.1}$$

$$H(C | \bar{C}) \leq \nabla(C) := H(C | A_{[e_n]}) + \sum_{i=1}^n I(A_{[e_n]-e_i}; C), \tag{A.2}$$

and for each $T \subseteq [e_n]$,

$$\begin{aligned}
 &H(A_e : e \in T | A'_e : e \in T) \leq \nabla(A_e : e \in T) \\
 &:= I(A_{[e_1, e_{k_1}]}; A_{[e_{k_1}, e_{k_2}]}) + \dots + I(A_{[e_1, e_{k_{l-1}}]}; A_{[e_{k_{l-1}}, e_{k_l}]}) .
 \end{aligned} \tag{A.3}$$

where e_{k_1}, \dots, e_{k_l} are in T with $k_1 \leq k_2 \leq \dots \leq k_l$ such that the intervals $[e_{k_1}, e_{k_2}), \dots, [e_{k_{l-1}}, e_{k_l}]$ are blocks, with maximum length, of a partition of T .

Proof: We first build mutually complementary subspaces $A'_{e_1}, \dots, A'_{e_n}$ in $A_{[e_n]}$ from A_1, \dots, A_n . Define $A'_{e_1} := A_{e_1}$, and for $i = 2, \dots, n$ denote by A'_{e_i} a subspace of A_i which is a complementary subspace to $A_{[e_{i-1}]}$ in $A_{[e_i]}$. Then $A'_{e_1}, \dots, A'_{e_n}$ are mutually complementary and the following equations hold:

$$H(A_{e_i} | A'_{e_i}) = I(A_{[e_{i-1}]}; A_{e_i}), \quad i = 1, \dots, n,$$

where $A_{e_0} := O$. Second, we built a subspace \bar{C} of $C \cap A'_{[e_n]}$ such that \bar{C} and $A'_{[e_n]-e_i}$ form a direct sum for all i . Let $C^{(0)} := C \cap A_{[e_n]}$. Recursively, for $i = 1, \dots, n$ denote by $C^{(i)}$ a subspace of $C^{(i-1)}$ which is a complementary subspace to $A'_{[e_n]-e_i}$ in $C^{(i-1)} + A'_{[e_n]-e_i}$. We denote $\bar{C} := C^{(n)}$, this space satisfies the required condition and the following inequalities:

$$H(C | C^{(0)}) \leq H(C | A_{[e_n]}),$$

$$H(C^{(0)} | \bar{C}) \leq \sum_{i=1}^n I(A_{[e_n]-e_i}; C).$$

These inequalities imply the bound on $H(C | \bar{C})$. For each $T \subseteq [e_n]$, the bound on $H(A_e : e \in T | A'_e : e \in T)$ is obtained from Lemma 3 in [8] and equations (A.1). \square

Remark A.1. *The tuple is not unique but we fix one of these.*

Lemma A.2. *Let A_{e_1}, \dots, 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, $(\bar{A}_{e_1}, \dots, \bar{A}_{e_n}, \bar{C})$ is a tuple of complementary vector subspaces that satisfies (i) in Lemma A.2 and

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

$$H(\bar{A}_{e_k}) = H(A_{e_k} | A_{[e_k-1]}), \text{ for } e_k \in \mathcal{B}',$$

$$H(A_{e_k} | \bar{A}_{e_k}) \leq H(A_{e_k}) - H(C) + \nabla(C), \text{ for } e_k \in \mathcal{B}''. \tag{A.4}$$

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

$$\bar{C} \leq \bigoplus_{e_i \notin \mathcal{B}''} A'_{e_i} + \bigoplus_{e_i \in \mathcal{B}'', i \leq k} \bar{A}_{e_i} + \bigoplus_{e_i \in \mathcal{B}'', i > k} A'_{e_i}. \tag{A.5}$$

In effect, we show case $k = l := \min \{i : e_i \in \mathcal{B}''\}$, 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 [7, Lemma 3], $c = \sum_i a_i$ 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, (A.5) 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 A.2. We also have the equation:

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

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

[from definition of mutual information and (A.5)]

$$= \mathbb{H}(\bar{C}). \quad [\text{definition of complementary subspaces}]$$

This last equation can be used to obtain the described upper bound on $\mathbb{H}(A_{e_k} | \bar{A}_{e_k})$. \square

Lemma A.3. Let $A_{e_1}, \dots, A_{e_n}, B_{e_{S_{j_1}}}, \dots, B_{e_{S_{j_{|\mathcal{B}'|}}}}$ 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 $\bar{A}_{e_1}, \dots, \bar{A}_{e_n}, \bar{B}_{e_{S_{j_1}}}, \dots, \bar{B}_{e_{S_{j_{|\mathcal{B}'|}}}}$ and \bar{C} satisfy hypothesis in Lemma A.2 and

$$\begin{aligned} \mathbb{H}(B_{e_{S_k}} | \bar{B}_{e_{S_k}}) &\leq \mathbb{H}(B_{e_{S_k}} | A_{e_i} : i \in S_k) + \mathbb{H}(B_{e_{S_k}} | A_{e_i}, C : i \notin S_k) + \sum_{e_i \in \mathcal{B}''} \mathbb{H}(A_{e_i}) \\ &+ \nabla(A_{e_i} : i \in S_k, e_i \notin \mathcal{B}'') + \nabla(A_{e_i} : i \notin S_k, e_i \notin \mathcal{B}'') + (|\mathcal{B}''| + 1) \nabla(C) - |\mathcal{B}''| \mathbb{H}(C) \end{aligned}$$

Proof: The conditions in Lemma A.2 are obviously true. To prove the inequality, we have

$$\begin{aligned} \mathbb{H}(B_{e_{S_k}} | \bar{B}_{e_{S_k}}) &\leq \mathbb{H}\left(B_{e_{S_k}} \mid \left(\bigoplus_{i \in S_k} \bar{A}_{e_i}\right) \cap B_{e_{S_k}}\right) + \mathbb{H}\left(B_{e_{S_k}} \mid \left[\bigoplus_{i \notin S_k} \bar{A}_{e_i} \oplus \bar{C}\right] \cap B_{e_{S_k}}\right) \\ &= \mathbb{H}\left(B_{e_{S_k}} \mid \left(\bigoplus_{i \in S_k} A_{e_i}\right) \cap B_{e_{S_k}}\right) + \mathbb{H}\left(B_{e_{S_k}} \mid \left[\bigoplus_{i \notin S_k} A_{e_i} \oplus C\right] \cap B_{e_{S_k}}\right) \\ &\quad + \mathbb{H}\left(\left(\sum_{i \in S_k} A_{e_i}\right) \cap B_{e_{S_k}} \mid \left(\bigoplus_{i \in S_k} \bar{A}_{e_i}\right) \cap B_{e_{S_k}}\right) \\ &\quad + \mathbb{H}\left(\left[\sum_{i \notin S_k} A_{e_i} \oplus C\right] \cap B_{e_{S_k}} \mid \left[\bigoplus_{i \notin S_k} \bar{A}_{e_i} \oplus \bar{C}\right] \cap B_{e_{S_k}}\right) \\ &\leq \mathbb{H}(B_{e_{S_k}} | A_{e_i} : i \in S_k) + \mathbb{H}(B_{e_{S_k}} | C, A_{e_i} : i \notin S_k) \\ &\quad + \mathbb{H}\left(\sum_{i \in S_k, e_i \in \mathcal{B}''} A_{e_i} \mid \bigoplus_{i \in S_k, e_i \in \mathcal{B}''} \bar{A}_{e_i}\right) + \mathbb{H}\left(\sum_{i \in S_k, e_i \notin \mathcal{B}''} A_{e_i} \mid \bigoplus_{i \in S_k, e_i \notin \mathcal{B}''} A'_{e_i}\right) + \\ &\quad \mathbb{H}\left(\sum_{i \notin S_k, e_i \in \mathcal{B}''} A_{e_i} \mid \bigoplus_{i \notin S_k, e_i \in \mathcal{B}''} \bar{A}_{e_i}\right) + \mathbb{H}\left(\sum_{i \notin S_k, e_i \notin \mathcal{B}''} A_{e_i} \mid \bigoplus_{i \notin S_k, e_i \notin \mathcal{B}''} A'_{e_i}\right) + \mathbb{H}(C | \bar{C}) \\ &\leq \mathbb{H}(B_{e_{S_k}} | A_{e_i} : i \in S_k) + \mathbb{H}(B_{e_{S_k}} | A_{e_i}, C : i \notin S_k) + \sum_{i \in S_k, e_i \in \mathcal{B}''} \mathbb{H}(A_{e_i}) \end{aligned}$$

$$\begin{aligned}
 &+ |\{e_i \in \mathcal{B}'' : i \in S_k\}| (\nabla(C) - H(C)) + \nabla(A_{e_i} : i \in S_k, e_i \notin \mathcal{B}'') + \sum_{i \notin S_k, e_i \in \mathcal{B}''} H(A_{e_i}) \\
 &+ |\{e_i \in \mathcal{B}'' : i \notin S_k\}| (\nabla(C) - H(C)) + \nabla(A_{e_i} : i \notin S_k, e_i \notin \mathcal{B}'') + \nabla(C)
 \end{aligned}$$

[from Lemmas 3 and 4 in [9], inequalities (A.3) and (A.4)].

$$\begin{aligned}
 &= H(B_{e_{S_k}} | A_{e_i} : i \in S_k) + H(B_{e_{S_k}} | A_{e_i}, C : i \notin S_k) + \sum_{e_i \in \mathcal{B}''} H(A_{e_i}) \\
 &+ (|\mathcal{B}''| + 1) \nabla(C) - |\mathcal{B}''| H(C) + \nabla(A_{e_i} : i \in S_k, e_i \notin \mathcal{B}'') + \nabla(A_{e_i} : i \notin S_k, e_i \notin \mathcal{B}'')
 \end{aligned}$$

□

Lemma A.4. Let $A_{e_1}, \dots, A_{e_n}, B_{e_{S_{j_1}}}, \dots, B_{e_{S_{j_{|\mathcal{B}'|}}}}$ 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

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

We have $A'_{e_1}, \dots, A'_{e_n}, \hat{B}_{e_{S_{j_1}}}, \dots, \hat{B}_{e_{S_{j_{|\mathcal{B}'|}}}}$ and \hat{C} satisfy hypothesis in Lemma A.3 and

$$H(B_{e_{S_k}} | \hat{B}_{e_{S_k}}) \leq H(B_{e_{S_k}} | A_{e_i} : i \in S_k) + \nabla(A_{e_i} : i \in S_k), \tag{A.6}$$

$$\begin{aligned}
 H(C | \hat{C}) &\leq \nabla(C) + \sum_{e_{S_k} \in \mathcal{B}'} \left[H(C | A_{e_i}, B_{S_k} : i \notin S_k) + H(B_{e_{S_k}} | A_{e_i} : i \in S_k) \right] \\
 &+ \sum_{e_{S_k} \in \mathcal{B}'} [\nabla(A_{e_i} : i \notin S_k) + \nabla(A_{e_i} : i \in S_k)]. \tag{A.7}
 \end{aligned}$$

Proof: By definition, we remark that $(A'_{e_1}, \dots, A'_{e_n}, \hat{C})$ is also a tuple of complementary vector subspaces and the other conditions in A.3 are also true. We only show last inequality:

$$\begin{aligned}
 H(C | \hat{C}) &\leq H(C | \bar{C}) + \sum_{e_{S_k} \in \mathcal{B}'} H\left(C | C \cap \left[\bigoplus_{i \notin S_k} A'_{e_i} + \hat{B}_{e_{S_k}} \right]\right) \\
 &= H(C | \bar{C}) + \sum_{e_{S_k} \in \mathcal{B}'} H\left(C | C \cap \left[\bigoplus_{i \notin S_k} A_{e_i} + B_{e_{S_k}} \right]\right) \\
 &+ \sum_{e_{S_k} \in \mathcal{B}'} H\left(C \cap \left[\sum_{i \notin S_k} A_{e_i} + B_{e_{S_k}} \right] | C \cap \left[\bigoplus_{i \notin S_k} A'_{e_i} + \hat{B}_{e_{S_k}} \right]\right) \\
 &\leq H(C | \bar{C}) + \sum_{e_{S_k} \in \mathcal{B}'} H\left(C | \bigoplus_{i \notin S_k} A_{e_i} + B_{e_{S_k}}\right) + \sum_{e_{S_k} \in \mathcal{B}'} H\left(\sum_{i \notin S_k} A_{e_i} | \bigoplus_{i \notin S_k} A'_{e_i}\right) \\
 &+ \sum_{e_{S_k} \in \mathcal{B}'} H(B_{e_{S_k}} | \hat{B}_{e_{S_k}}) \text{ [from Lemmas 3 and 4 in [8] and inequality (A.6)]}
 \end{aligned}$$

$$\begin{aligned} &\leq \nabla(C) + \sum_{e_{S_k} \in \mathcal{B}'} \left[\mathbb{H}(C \mid A_{e_i}, B_{S_k} : i \notin S_k) + \mathbb{H}(B_{e_{S_k}} \mid A_{e_i} : i \in S_k) \right] \\ &+ \sum_{e_{S_k} \in \mathcal{B}'} [\nabla(A_{e_i} : i \notin S_k) + \nabla(A_{e_i} : i \in S_k)] \text{ [from (A.3)]} \end{aligned}$$

□

We finally prove the main theorem.

Proof of Theorem 2.1: By Lemmas A.2 and A.3, the subspaces $\bar{A}_{e_1}, \dots, \bar{A}_{e_n}, \bar{B}_{e_{S_{j_1}}}, \dots, \bar{B}_{e_{S_{j_{|\mathcal{B}'|}}}}$ and \bar{C} satisfy hypothesis of the Proposition A.2 in a finite field \mathbb{F} whose characteristic divides t_k , we get

$$\mathbb{H}(\bar{B}_{e_{S_i}}, \bar{A}_{e_j}, \bar{C} : e_{S_i} \in \mathcal{B}', e_j \in \mathcal{B}'', \bar{C} \in \mathcal{B}''') \leq m_k \mathbb{H}(\bar{C}). \tag{A.8}$$

On the other hand,

$$\mathbb{H}(\bar{C}) \leq \mathbb{I}(A_{[e_n]}; C) \text{ [from } \bar{C} \leq C], \tag{A.9}$$

$$\mathbb{H}\left(\sum_{e_{S_k} \in \mathcal{B}'} B_{S_i} \mid \sum_{e_{S_k} \in \mathcal{B}'} \bar{B}_{S_1}\right) \leq \sum_{e_{S_k} \in \mathcal{B}'} \mathbb{H}(B_{e_{S_i}} \mid \bar{B}_{e_{S_i}}) \text{ [from Lemma 3 in [8]].}$$

Therefore,

$$\begin{aligned} &\mathbb{H}\left(\sum_{e_{S_k} \in \mathcal{B}'} B_{S_i} + \sum_{e_i \in \mathcal{B}''} A_{e_i} + C \mid \sum_{e_{S_k} \in \mathcal{B}'} \bar{B}_{S_i} + \sum_{e_i \in \mathcal{B}''} \bar{A}_{e_i} + \bar{C}\right) \leq \sum_{e_{S_k} \in \mathcal{B}'} \mathbb{H}(B_{e_{S_k}} \mid A_{e_i} : i \in S_k) \\ &+ \sum_{e_{S_k} \in \mathcal{B}'} \mathbb{H}(B_{e_{S_k}} \mid A_{e_i}, C : i \notin S_k) + (|\mathcal{B}'| + 1) \sum_{e_i \in \mathcal{B}''} \mathbb{H}(A_{e_i}) \\ &+ (|\mathcal{B}''| |\mathcal{B}'| + |\mathcal{B}''| + |\mathcal{B}'| + 1) \nabla(C) - (|\mathcal{B}''| |\mathcal{B}'| + |\mathcal{B}''|) \mathbb{H}(C) \\ &+ \sum_{e_{S_k} \in \mathcal{B}'} [\nabla(A_{e_i} : i \in S_k, e_i \notin \mathcal{B}'') + \nabla(A_{e_i} : i \notin S_k, e_i \notin \mathcal{B}'')]. \end{aligned}$$

From (A.8), (A.9), (A.2) 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 $k = 1, \dots, s$. Noting that inequality (A.8) 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 A.4, the vector subspaces $A'_{e_1}, \dots, A'_{e_n}, \hat{B}_{e_{S_{j_1}}}, \dots, \hat{B}_{e_{S_{j_{|\mathcal{B}'|}}}}$ and \hat{C} satisfy hypothesis of Proposition A.3 in a finite field \mathbb{F} whose characteristic does not divide t , we get

$$m\mathbb{H}(\hat{C}) \leq \mathbb{H}(A'_{e_i}, \hat{B}_{e_{S_j}}, \hat{C} : e_{S_j} \in \mathcal{B}', e_i \in \mathcal{B}'', \hat{C} \in \mathcal{B}'''). \tag{A.10}$$

On the other hand,

$$\mathbb{H}(A'_{e_i}, \hat{B}_{e_{S_j}}, \hat{C} : e_{S_j} \in \mathcal{B}', e_i \in \mathcal{B}'', \hat{C} \in \mathcal{B}''') \leq \mathbb{H}(A_{e_i}, B_{e_{S_j}}, C : e_{S_j} \in \mathcal{B}', e_i \in \mathcal{B}'', C \in \mathcal{B}'''). \tag{A.11}$$

From (A.10), (A.7) and last inequality, we can derive the inequality (ii) over fields whose characteristic does not divide t . □