Groups and information inequalities in 5 variables

Markin, Nadya; Thomas, Eldho; Oggier, Frederique

2013

Markin, N., Thomas, E., & Oggier, F. (2013). Groups and information inequalities in 5 variables. 2013 51st Annual Allerton Conference on Communication, Control, and Computing (Allerton), 804 - 809.

<https://hdl.handle.net/10356/97296>

<https://doi.org/10.1109/Allerton.2013.6736607>

© 2013 IEEE. This is the author created version of a work that has been peer reviewed and accepted for publication by 2013 51st Annual Allerton Conference on Communication, Control, and Computing (Allerton), IEEE. It incorporates referee's comments but changes resulting from the publishing process, such as copyediting, structural formatting, may not be reflected in this document. The published version is available at:
[DOI:<http://dx.doi.org/10.1109/Allerton.2013.6736607>].

Downloaded on 26 Apr 2023 16:43:48 SGT

Groups and Information Inequalities in 5 Variables

Nadya Markin, Eldho Thomas, Frédérique Oggier

Division of Mathematical Sciences

Nanyang Technological University

Singapore

Email: nmarkin@ntu.edu.sg, eldho1@e.ntu.edu.sg, frederique@ntu.edu.sg

Abstract—Linear rank inequalities in 4 subspaces are characterized by Shannon-type inequalities and the Ingleton inequality in 4 random variables. Examples of random variables violating these inequalities have been found using finite groups, and are of interest for their applications in nonlinear network coding [1]. In particular, it is known that the symmetric group S_5 provides the first instance of a group, which gives rise to random variables that violate the Ingleton inequality. In the present paper, we are interested in investigating inequalities in 5 random variables. In this case, linear rank inequalities are described using not only Shannon-type inequalities together with 4 Ingleton inequalities, but also 24 additional inequalities. We continue the study of finite groups as a way of finding random variables which violate one of these inequalities. To begin tackling the problem, we focus on 2 of the 24 additional inequalities in 5 random variables and formulate conditions for finite groups which help us eliminate those groups that obey the 2 inequalities. In particular, we show that groups of order pq , where p, q are prime, always satisfy them, and exhibit the first violator, which is the symmetric group S_4 .

I. INTRODUCTION

An information inequality is a linear inequality involving entropies of jointly distributed random variables. We will be interested in information inequalities which always hold, for any joint distribution of the random variables involved. There are two types of such inequalities: the Shannon-type inequalities (those that can be derived from the non-negativity of the conditional mutual information $I(A; B|C) \geq 0$, where A, B, C each denote the joint distribution of some arbitrary, possibly empty, subset of the random variables involved), and the non-Shannon-type inequalities [2, Chap. 13].

A linear rank inequality is a linear inequality involving the rank of subspaces of a (finite) vector space over some field F . Connections between linear rank and information inequalities that always hold have been classically studied. Indeed, there is a natural translation of entropy and mutual information in terms of rank: for A, B, C either random variables or subspaces, $H(A)$ is the entropy of A , or the rank of A , $H(A, B)$ is the joint entropy of A and B , or the rank of the span $\langle A, B \rangle$ of A and B , the mutual information

$$I(A; B) = H(A) + H(B) - H(A, B)$$

is the rank of $A \cap B$, the conditional entropy $H(A|B) = H(A, B) - H(B)$ is the excess of the rank of A over that of $A \cap B$, and the conditional mutual information

$$I(A; B|C) = H(A, C) + H(B, C) - H(A, B, C) - H(C)$$

is the excess of the rank of $(A + C) \cap (B + C)$ over that of C . The non-negativity of the conditional mutual information holds in both interpretations, and so does the non-negativity of the mutual information and of the conditional entropy.

It was shown in [3] that any linear information inequality that always holds is also a linear rank inequality which always holds for finite dimensional vector spaces over F . The converse is not true: the Ingleton inequality [4]

$$I(A; B) \leq I(A; B|C) + I(A; B|D) + I(C; D) \quad (1)$$

always holds for ranks of subspaces, yet does not hold for random variables. Examples of random variables whose joint entropies do not satisfy Ingleton were given by Matúš in [5]. Furthermore, it is known [3] that the Ingleton inequality, together with its permuted variable forms, and the Shannon-type inequalities fully characterize linear rank inequalities on 4 subspaces (or random variables).

For 5 subspaces (or random variables), the situation gets more complicated [6]: this time, the Shannon-type inequalities, 4 Ingleton inequalities (see (3) below for a description of what these are), and 24 new inequalities are needed to fully characterize all the linear rank inequalities.

Finding 4 random variables violating the Ingleton is not easy. Examples using group theory were found in [1].

This paper extends the approach of [1] to the case of 5 random variables. Firstly, we prove in Section II that random variables from finite groups violate the Ingleton inequality for 4 random variables if and only they violate the Ingleton inequalities for 5 random variables. How finite groups give rise to random variables will be recalled in the same section. We then consider 2 of the 24 new inequalities in Section III. We provide sufficient conditions for finite groups to satisfy them, in particular we prove that groups of order pq , where p, q are two primes, never violate these 2 inequalities. We also demonstrate that the smallest group violating the first inequality is the symmetric group S_4 of order 24. This comes as a surprise, compared to the case of 4 random variables, where the first instance of group that yields a violation of the Ingleton inequality has order 120.

II. INGLETON INEQUALITIES

A. Minimal Set of Ingleton Inequalities

Let $\mathcal{N} = \{1, \dots, n\}$ induce a 2^{n-1} -dimensional real Euclidean space whose coordinates are indexed by the set of all nonempty subsets $\mathcal{A} \subseteq \mathcal{N}$. Points in this space may also

be considered as functions from $2^{\mathcal{N}}$ to $\mathbb{R}$, in which case it is assumed that the empty set is mapped to 0. The entropy H of n jointly distributed discrete random variables $X_1, \dots, X_n$, is such a function. Set $X_{\mathcal{A}} = \{X_i, i \in \mathcal{A}\}$.

Definition 1. [7] An *Ingleton inequality* $J(H; \mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \mathcal{A}_4) \geq 0$ is a linear inequality defined in terms of four subsets $\mathcal{A}_1, \dots, \mathcal{A}_4 \subseteq \mathcal{N}$ where

$$\begin{aligned} J(H; \mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \mathcal{A}_4) &= H(X_{\mathcal{A}_1 \cup \mathcal{A}_2}) + H(X_{\mathcal{A}_1 \cup \mathcal{A}_3}) + H(X_{\mathcal{A}_1 \cup \mathcal{A}_4}) - H(X_{\mathcal{A}_1}) \\ &\quad + H(X_{\mathcal{A}_2 \cup \mathcal{A}_4}) + H(X_{\mathcal{A}_2 \cup \mathcal{A}_3}) - H(X_{\mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{A}_3}) \\ &\quad - H(X_{\mathcal{A}_3 \cup \mathcal{A}_4}) - H(X_{\mathcal{A}_2}) - H(X_{\mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{A}_4}). \end{aligned} \quad (2)$$

The notation $J(H; \mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \mathcal{A}_4)$ suggests that an Ingleton inequality could be defined on a function different from H .

Since the subsets $\mathcal{A}_1, \dots, \mathcal{A}_4$ are arbitrary, some inequalities are redundant, and Guille et al. [7] computed the minimal set of Ingleton inequalities, that is, the (unique) set of Ingleton inequalities which describes all of them without redundancy.

Example 1. When $n = 4$, there is one Ingleton inequality, already mentioned in (1), which can be rephrased in terms of conditional mutual information as:

$$I(X_1; X_2) \leq I(X_1; X_2 | X_3) + I(X_1; X_2 | X_4) + I(X_3; X_4).$$

It will be referred to as the 4-Ingleton inequality for short.

Example 2. When $n = 5$, the following three 5-Ingleton inequalities expressed in terms of conditional mutual information form a minimal set of Ingleton inequalities [6], together with the 4-Ingleton inequality:

$$\begin{aligned} I(X_1; X_2) &\leq I(X_1; X_2 | X_3) + I(X_3; X_4, X_5) \\ &\quad + I(X_1; X_2 | X_4, X_5) \\ I(X_1; X_2, X_3) &\leq I(X_1; X_2, X_3 | X_4) + I(X_4; X_5) \\ &\quad + I(X_1; X_2, X_3 | X_5) \\ I(X_1, X_2; X_1, X_3) &\leq I(X_1, X_2; X_1, X_3 | X_1, X_4) \\ + I(X_1, X_4; X_1, X_5) &+ I(X_1, X_2; X_1, X_3 | X_1, X_5). \end{aligned} \quad (3)$$

B. Group Theoretic Formulation of Ingleton Inequalities

Let G be a finite group and $G_1, \dots, G_n$ be subgroups of G . We denote by $G_{\mathcal{A}} = \cap_{i \in \mathcal{A}} G_i$ the subgroup formed by intersecting G_i where $i \in \mathcal{A}$.

Let X be a random variable uniformly distributed over G , that is $P(X = g) = 1/|G|$, for any $g \in G$. Define the new random variable $X_i = XG_i$, with support the $[G : G_i]$ cosets of G_i in G . Then $P(X_i = gG_i) = |G_i|/|G|$ and $P(X_i = gG_i, i \in \mathcal{A}) = |\cap_{i \in \mathcal{A}} G_i|/|G|$. More precisely:

Theorem 1. [8] For any finite group G and any subgroups $G_1, \dots, G_n$ of G , there exist n jointly distributed quasi-uniform discrete random variables $X_1, \dots, X_n$ such that for all non-empty subsets $\mathcal{A}$ of $\mathcal{N}$, $P(X_{\mathcal{A}} = x_{\mathcal{A}}) = |G_{\mathcal{A}}|/|G|$.

We then have that

$$H(X_{\mathcal{A}}) = \log(|G|/|G_{\mathcal{A}}|),$$

which can be used to rewrite (2) in terms of groups as:

$$\begin{aligned} J(H; \mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \mathcal{A}_4) \geq 0 &\iff \\ |G_{\mathcal{A}_1 \cup \mathcal{A}_2}| |G_{\mathcal{A}_1 \cup \mathcal{A}_3}| |G_{\mathcal{A}_1 \cup \mathcal{A}_4}| |G_{\mathcal{A}_2 \cup \mathcal{A}_3}| |G_{\mathcal{A}_2 \cup \mathcal{A}_4}| & \\ \leq |G_{\mathcal{A}_1}| |G_{\mathcal{A}_2}| |G_{\mathcal{A}_3 \cup \mathcal{A}_4}| |G_{\mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{A}_3}| |G_{\mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{A}_4}|. \end{aligned} \quad (4)$$

Definition 2. We say that a finite group G violates the n -Ingleton inequality (4) if it contains n subgroups $G_1, \dots, G_n$ such that (4) does not hold.

Example 3. We get the 4-Ingleton inequality

$$|G_{12}| |G_{13}| |G_{14}| |G_{23}| |G_{24}| \leq |G_1| |G_2| |G_{34}| |G_{123}| |G_{124}| \quad (5)$$

from Example 1. Examples of groups violating this inequality were studied in [1], [9], [10].

We are interested in groups violating the 5-Ingleton inequalities, which, from Example 2, are

$$\begin{aligned} |G_{12}| |G_{13}| |G_{145}| |G_{23}| |G_{245}| &\leq \\ |G_1| |G_2| |G_{345}| |G_{123}| |G_{1245}| & \end{aligned} \quad (6)$$

$$\begin{aligned} |G_{123}| |G_{14}| |G_{15}| |G_{235}| |G_{234}| &\leq \\ |G_1| |G_{23}| |G_{54}| |G_{1235}| |G_{1234}| & \end{aligned} \quad (7)$$

$$\begin{aligned} |G_{123}| |G_{124}| |G_{125}| |G_{134}| |G_{135}| &\leq \\ |G_{12}| |G_{13}| |G_{145}| |G_{1234}| |G_{1235}| & \end{aligned} \quad (8)$$

and the 4-Ingleton inequality (5). Note first that both (6) and (7) in isolation can be reduced to the 4-Ingleton inequality. Indeed, take (6) and set $G_6 = G_{45}$, then (6) becomes

$$|G_{12}| |G_{13}| |G_{16}| |G_{23}| |G_{26}| \leq |G_1| |G_2| |G_{36}| |G_{123}| |G_{126}|,$$

which is (5) with a change of labels. Similarly, set $G_6 = G_{23}$ in (7), which becomes again (5) with a change of labels.

Now when $G_1 = G$, (7) becomes the Ingleton inequality for 4 random variables, so

$$\begin{aligned} |G_{123}| |G_{124}| |G_{125}| |G_{134}| |G_{135}| &\leq \\ |G_{12}| |G_{13}| |G_{145}| |G_{1234}| |G_{1235}| & \end{aligned}$$

looks like a stronger inequality. It is, however, easy to see that looking for a finite group which violates inequalities in (5)-(8) reduces to looking for a violator of the 4-Ingleton inequality. We detail this in the following lemma.

Lemma 1. If a group G does not violate the 4-Ingleton inequality (1), then it does not violate any of the four 5-Ingleton inequalities, i.e., the inequalities in (5)-(8) are simultaneously satisfied. On the other hand if G obeys all 5-Ingleton inequalities for all subgroups $G_1, \dots, G_5 \in G$, then G obeys the 4-Ingleton inequality for all subgroups $G_1, \dots, G_4 \in G$.

Proof: Fix arbitrary subgroups $G_1, G_2, G_3, G_4, G_5 \leq G$. The inequalities in (5)-(6) correspond to the following

4-Ingelton inequalities on different subgroups

$$\begin{aligned} J(H; 1, 2, 3, 4) &\geq 0 \\ J(H; 1, 2, 3, \{45\}) &\geq 0 \\ J(H; 1, \{23\}, 5, 4) &\geq 0 \\ J(H; \{12\}, \{13\}, \{14\}, \{15\}) &\geq 0 \end{aligned}$$

Since by assumption the group G does not violate the 4-Ingelton inequality (5) for any choice of subgroups $A, B, C, D \leq G$, the 4 inequalities above must all be satisfied.

The converse is clear since the first 5-Ingelton inequality is the 4-Ingelton inequality. ■

III. OTHER INEQUALITIES ON 5 VARIABLES

It was shown in [6] that linear rank inequalities for $n = 5$ random variables are characterized by Shannon-type inequalities, the Ingelton inequalities (5)-(8), and 24 other inequalities. The first two of them are

$$\begin{aligned} I(X_1; X_2) &\leq I(X_1; X_2|X_3) + I(X_1; X_2|X_4) \\ &\quad + I(X_3; X_4|X_5) + I(X_1; X_5) \end{aligned} \quad (9)$$

$$\begin{aligned} I(X_1; X_2) &\leq I(X_1; X_2|X_3) + I(X_1; X_3|X_4) \\ &\quad + I(X_1; X_4|X_5) + I(X_2; X_5) \end{aligned} \quad (10)$$

Similarly to Definition 2, we say that a group G violates the inequality (9), or (10), if G contains n subgroups $G_1, \dots, G_n$ such that (9), or (10), does not hold.

To find violating groups, it is useful to have conditions which guarantee that a group (or its chosen subgroups) will not result in a violation. For the 4-Ingelton inequality, the following conditions are all sufficient to tell when chosen subgroups $G_1, \dots, G_4$ of G will not result in a violation of the 4-Ingelton inequality:

- All G_i are normal.
- $G_1 G_2 = G_2 G_1$.
- $G_i = \{1\}$ or $G_i = G$ for some i .
- $G_i = G_j$ for some $i \neq j$.
- $G_{12} = \{1\}$.
- $G_i \leq G_j$ for some $i \neq j$.

We will extend some of these conditions to the two inequalities considered. We will make extensive use of the following lemma, which rephrases non-negativity of conditional mutual information in terms of subgroup intersections.

Lemma 2. *Let G be a finite group with n subgroups $G_1, \dots, G_n$. For any choice of subsets $\mathcal{A}_2, \mathcal{A}_3, \mathcal{A}_4$ of $\mathcal{N}$*

$|G_{\mathcal{A}_2 \cup \mathcal{A}_3}| |G_{\mathcal{A}_2 \cup \mathcal{A}_4}| \leq |G_{\mathcal{A}_2}| |G_{\mathcal{A}_2 \cup \mathcal{A}_3 \cup \mathcal{A}_4}| \leq |G_{\mathcal{A}_2}| |G_{\mathcal{A}_3 \cup \mathcal{A}_4}|$
is always satisfied.

Proof: Since $G_{\mathcal{A}_2 \cup \mathcal{A}_3}$ and $G_{\mathcal{A}_2 \cup \mathcal{A}_4}$ are subgroups of $G_{\mathcal{A}_2}$

$$|G_{\mathcal{A}_2 \cup \mathcal{A}_3}| |G_{\mathcal{A}_2 \cup \mathcal{A}_4}| \leq |G_{\mathcal{A}_2}| |G_{\mathcal{A}_2 \cup \mathcal{A}_3 \cup \mathcal{A}_4}| \leq |G_{\mathcal{A}_2}| |G_{\mathcal{A}_3 \cup \mathcal{A}_4}|.$$

To see the first inequality, recall from [11] that one can define a map $f : G_{\mathcal{A}_2 \cup \mathcal{A}_3} \times G_{\mathcal{A}_2 \cup \mathcal{A}_4} \rightarrow G_{\mathcal{A}_2}$ that sends (h, k) to hk . Then $f(G_{\mathcal{A}_2 \cup \mathcal{A}_3} \times G_{\mathcal{A}_2 \cup \mathcal{A}_4}) \simeq G_{\mathcal{A}_2} / G_{\mathcal{A}_2 \cup \mathcal{A}_3 \cap \mathcal{A}_4}$. ■

A. Conditions of the Form $G_i \leq G_j$ and $G_i = \{1\}$

First rewrite the inequalities (9) and (10) respectively as

$$\begin{aligned} I(X_1; X_2) - I(X_1; X_5) &\leq \\ I(X_1; X_2|X_3) + I(X_1; X_2|X_4) + I(X_3; X_4|X_5), \\ I(X_1; X_2) - I(X_2; X_5) &\leq \\ I(X_1; X_2|X_3) + I(X_1; X_3|X_4) + I(X_1; X_4|X_5). \end{aligned}$$

Expressed in terms of groups as done in the case of Ingelton before, these inequalities correspond respectively to

$$\frac{|G||G_{12}||G_1||G_5|}{|G_1||G_2||G||G_{15}|} \leq \frac{|G_3||G_{123}||G_4||G_{124}||G_5||G_{345}|}{|G_{13}||G_{23}||G_{14}||G_{24}||G_{35}||G_{45}|} \quad (11)$$

$$\frac{|G||G_{12}||G_2||G_5|}{|G_1||G_2||G||G_{25}|} \leq \frac{|G_3||G_{123}||G_4||G_{134}||G_5||G_{145}|}{|G_{13}||G_{23}||G_{14}||G_{34}||G_{15}||G_{45}|} \quad (12)$$

The following lemma is now immediate:

Lemma 3. *Suppose $G_5 \leq G_1$, then the inequality (9) holds. Suppose $G_5 \leq G_2$, then the inequality (10) holds.*

Proof: Observe that by Lemma 2 each of the three products in the RHS of (11) and (12) are ≥ 1 , while the assumptions guarantee that LHS of (11) (resp. (12)) is ≤ 1 . ■

Next, simplify inequality (11) and (12) respectively to

$$\begin{aligned} |G_{12}||G_{13}||G_{23}||G_{14}||G_{24}||G_{35}||G_{45}| &\leq \\ |G_2||G_3||G_{123}||G_{15}||G_{124}||G_4||G_{345}| \end{aligned} \quad (13)$$

$$\begin{aligned} |G_{12}||G_{13}||G_{23}||G_{14}||G_{34}||G_{15}||G_{45}| &\leq \\ |G_1||G_3||G_{123}||G_{25}||G_{134}||G_4||G_{145}|. \end{aligned} \quad (14)$$

Finding finite groups violating these inequalities using a computer search can be computationally costly as the size of the group increases. The following lemma can be used in order to simplify the search.

Lemma 4. *The inequality (13) holds if any of the following conditions hold*

$$G_1 \leq G_{25}, G_2 \leq G_1, G_3 \leq G_4, G_4 \leq G_3.$$

The inequality (14) holds if any one of the following hold:

$$G_1 \leq G_{34}, G_2 \leq G_5, G_3 \leq G_1, G_4 \leq G_1.$$

Proof:

1) *Conditions on G_1 :* We break the inequality (13) into two inequalities, the first one containing terms involving G_1 and the second inequality not involving G_1 :

$$\begin{aligned} |G_{12}||G_{13}||G_{14}| &\leq |G_{123}||G_{15}||G_{124}|, \\ |G_{23}||G_{24}||G_{35}||G_{45}| &\leq |G_2||G_3||G_4||G_{345}|. \end{aligned}$$

If each of the inequalities above holds, then so does (13). Consider the inequality not involving G_1 . By Lemma 2

$$\begin{aligned} (|G_{23}||G_{24}|)|G_{35}||G_{45}| &\leq |G_2|(|G_{234}||G_{35}|)|G_{45}| \\ &\leq |G_2||G_3|(|G_{2345}||G_{45}|) \\ &\leq |G_2||G_3||G_4||G_{2345}| \\ &\leq |G_2||G_3||G_4||G_{345}|, \end{aligned}$$

the RHS of (13) without terms in G_1 . Hence to satisfy (13), it is enough for the inequality with terms in G_1 to hold:

$$|G_{12}||G_{13}||G_{14}| \leq |G_{15}||G_{123}||G_{124}|.$$

Now if $G_1 \leq G_{25}$, then $G_1 \leq G_2$ and $G_1 \leq G_5$, and

$$|G_{12}||G_{13}||G_{14}| = |G_1||G_{13}||G_{14}| = |G_{15}||G_{123}||G_{124}|.$$

2) *Conditions on G_2* : The LHS of inequality (13) without terms having G_2 is

$$\begin{aligned} (|G_{13}||G_{35}|)(|G_{14}||G_{45}|) &\leq |G_3||G_4|(|G_{135}||G_{145}|) \\ &\leq |G_3||G_4|(|G_{15}||G_{1345}|) \\ &\leq |G_3||G_4||G_{15}||G_{345}|, \end{aligned}$$

the RHS without terms in G_2 . It is then enough that $|G_{12}||G_{23}||G_{24}| \leq |G_2||G_{123}||G_{124}|$ in order for (13) to be satisfied. By Lemma 2, we only need $|G_{24}| \leq |G_{124}|$, which holds when $G_2 \leq G_1$.

3) *Conditions on G_3* : By avoiding terms in G_3 from (13)

$$\begin{aligned} (|G_{12}||G_{24}|)(|G_{14}||G_{45}|) &\leq |G_2||G_4|(|G_{124}||G_{145}|) \\ &\leq |G_2||G_4||G_{124}||G_{15}|. \end{aligned}$$

It thus suffices to have $|G_{13}||G_{23}||G_{35}| \leq |G_3||G_{123}||G_{345}|$ for (13) to hold. Now Lemma 2 yields $G_3 \leq G_4$ as the sufficient condition.

4) *Conditions on G_4* : Similarly

$$\begin{aligned} (|G_{12}||G_{23}|)(|G_{13}||G_{35}|) &\leq |G_2||G_{123}||G_3||G_{135}| \\ &\leq |G_2||G_3||G_{123}||G_{15}|, \end{aligned}$$

after omitting terms in G_4 from the LHS, and $|G_{14}||G_{24}||G_{45}| \leq |G_4||G_{124}||G_{345}|$ is a sufficient condition for (13) to hold, which is true when $G_4 \leq G_3$.

A similar proof shows the results for the second inequality. ■

Corollary 1. *If any $G_i = \{1\}$, then both (13) and (14), and hence (9) and (10), always hold.*

Proof: If $G_i = \{1\}$ for any $i = 1, \dots, 5$, then $G_i \leq G_j$ for all j , hence satisfying the condition of Lemma 4. The result follows. ■

B. Groups of Order pq

The following two lemmas give a class of groups which never violate inequalities (9), (10).

Lemma 5. *If G is a group such that any two of its distinct proper subgroups intersect trivially, then G does not violate (9).*

Proof: We consider two cases.

Case 1. Suppose $|G_{12}| \neq 1$, which under the assumption about our group G occurs only when $G_1 = G_2$. Then the inequality (13), which we need to show, simplifies to

$$|G_{13}||G_{14}||G_{35}||G_{45}| \leq |G_{15}||G_3||G_4||G_{345}|.$$

Now we apply Lemma 2 repeatedly (indicated by parenthesis around relevant terms) to show

$$\begin{aligned} |G_{13}||G_{14}||G_{35}||G_{45}| &= (|G_{13}||G_{35}|)(|G_{14}||G_{45}|) \leq \\ |G_3||G_{135}||G_4||G_{145}| &= (|G_{135}||G_{145}|)|G_3||G_4| \leq \\ (|G_{15}||G_{1345}|)|G_3||G_4| &\leq |G_{15}||G_{345}||G_3||G_4| \end{aligned}$$

as desired.

Case 2. Next we consider the case $G_{12} = \{1\}$, i.e., $G_1 \neq G_2$. Then the inequality (13) simplifies to

$$|G_{13}||G_{23}||G_{14}||G_{24}||G_{35}||G_{45}| \leq |G_3||G_4||G_{345}||G_2||G_{15}| \quad (15)$$

We apply Lemma 2 repeatedly to a rearranged LHS to get

$$\begin{aligned} (|G_{13}||G_{35}|)(|G_{23}||G_{24}|)(|G_{14}||G_{45}|) &\leq \\ |G_3||G_{135}||G_2||G_{234}||G_4||G_{145}| &= \\ (|G_{135}||G_{145}|)|G_{234}||G_3||G_2||G_4| &\leq \\ |G_{15}||G_{1345}||G_{234}||G_3||G_2||G_4| &= \\ |G_{15}|(|G_{1345}||G_{234}|)|G_3||G_2||G_4| &\leq \\ |G_{15}||G_{34}||G_{1234}||G_3||G_2||G_4| &= \\ |G_{15}||G_{34}||G_3||G_2||G_4|. \end{aligned}$$

If $|G_{34}| \leq |G_{345}|$, then we have shown inequality (15).

It hence remains to consider the case $G_{345} < G_{34}$. Recalling the assumption on the group G , this can only happen when $G_3 = G_4 \neq G_5$. Together with the original assumption that $|G_{12}| = 1$ the inequality (13) simplifies to

$$|G_{13}||G_{23}||G_{13}||G_{23}| \leq |G_3||G_3||G_2||G_{15}|$$

which follows since

$$(|G_{13}||G_{23}|)|G_{13}||G_{23}| \leq |G_3||G_{123}||G_3||G_{123}| = |G_3||G_3|. \quad \blacksquare$$

We proceed to show that the same class of groups does not violate inequality (10).

Lemma 6. *Let G be a group with the property that any two of its distinct proper subgroups intersect trivially. Then G does not violate (10).*

Proof: First recall that (10) can be written as

$$\begin{aligned} I(X_1; X_2) - I(X_2; X_5) &\leq \\ I(X_1; X_2|X_3) + I(X_1; X_3|X_4) + I(X_1; X_4|X_5). \end{aligned}$$

and expressed in terms of groups, it corresponds to

$$\frac{|G_{12}|}{|G_1|} \frac{|G_5|}{|G_{25}|} \leq \frac{|G_3||G_{123}|}{|G_{13}||G_{23}|} \frac{|G_4||G_{134}|}{|G_{14}||G_{34}|} \frac{|G_5||G_{145}|}{|G_{15}||G_{45}|}. \quad (16)$$

Let us first analyze the term $\frac{|G_3||G_{123}|}{|G_{13}||G_{23}|}$ corresponding to $I(X_1; X_2|X_3)$. Recall the assumption that two proper subgroups of G are either distinct or have trivial intersection. With that in mind, we have the following observation

$$\frac{|G_3||G_{123}|}{|G_{13}||G_{23}|} = \begin{cases} 1, & G_1 = G_3 \\ 1, & G_2 = G_3 \\ |G_3|, & \text{otherwise} \end{cases} \quad (17)$$

Similar observations hold for terms $\frac{|G_4||G_{134}|}{|G_{14}||G_{34}|}$, $\frac{|G_5||G_{145}|}{|G_{15}||G_{45}|}$, and will also be referred to as observation (17). From this we see that the RHS of (16) is a divisor of $|G_3||G_4||G_5|$ with $\frac{|G_3||G_{123}|}{|G_{13}||G_{23}|}$, $\frac{|G_4||G_{134}|}{|G_{14}||G_{34}|}$, $\frac{|G_5||G_{145}|}{|G_{15}||G_{45}|}$ possibly contributing to each (and only one) of the terms $|G_3|$, $|G_4|$, $|G_5|$ respectively. Based on this observation, we now consider various cases.

a) Suppose $|G_5|$ divides the RHS of (16): This can only happen when $\frac{|G_5||G_{145}|}{|G_{15}||G_{45}|} = |G_5|$. Then (16) becomes

$$\frac{|G_{12}|}{|G_1|} \frac{|G_5|}{|G_{25}|} \leq \frac{|G_3||G_{123}|}{|G_{13}||G_{23}|} \frac{|G_4||G_{134}|}{|G_{14}||G_{34}|} |G_5|. \quad (18)$$

Noting that the first two products in the RHS are ≥ 1 , it suffices to show

$$\frac{|G_{12}|}{|G_1|} \frac{|G_5|}{|G_{25}|} \leq |G_5|, \quad (19)$$

which is obviously true.

b) Now suppose $|G_5|$ does not divide the RHS of (16): In other words, $\frac{|G_5||G_{145}|}{|G_{15}||G_{45}|} = 1$.

By observation (17) this only happens when either $G_5 = G_4$ or $G_5 = G_1$. Then (16) becomes

$$\frac{|G_{12}|}{|G_1|} \frac{|G_5|}{|G_{25}|} \leq \frac{|G_3||G_{123}|}{|G_{13}||G_{23}|} \frac{|G_4||G_{134}|}{|G_{14}||G_{34}|} \cdot 1 \quad (20)$$

We treat the cases $G_5 = G_4$ and $G_5 = G_1$ below:

1) Suppose $G_5 = G_1$: Then the LHS of the inequality above is 1 and we are done, since RHS is always ≥ 1 (each of the three products of the RHS is ≥ 1 by Lemma 2.)

2) Suppose $G_5 = G_4$: Then the inequality above becomes

$$\frac{|G_{12}|}{|G_1|} \frac{|G_4|}{|G_{24}|} \leq \frac{|G_3||G_{123}|}{|G_{13}||G_{23}|} \frac{|G_4||G_{134}|}{|G_{14}||G_{34}|} \cdot 1 \quad (21)$$

Apply observation (17) to the second term $\frac{|G_4||G_{134}|}{|G_{14}||G_{34}|}$.

If $\frac{|G_4||G_{134}|}{|G_{14}||G_{34}|} = |G_4|$, we are finished by canceling the term $|G_4|$ on both sides.

It is left to consider the case when $\frac{|G_4||G_{134}|}{|G_{14}||G_{34}|} = 1$, which by (17) happens when $G_3 = G_4$ or $G_1 = G_4$. The inequality above becomes

$$\frac{|G_{12}|}{|G_1|} \frac{|G_4|}{|G_{24}|} \leq \frac{|G_3||G_{123}|}{|G_{13}||G_{23}|} \cdot 1 \cdot 1 \quad (22)$$

If $G_1 = G_4$, then the LHS of the inequality above is 1 and we are done.

If $G_3 = G_4$, then rewriting the inequality above gives

$$\frac{|G_{12}|}{|G_1|} \frac{|G_3|}{|G_{23}|} \leq \frac{|G_3||G_{123}|}{|G_{13}||G_{23}|} \cdot 1 \cdot 1 \quad (23)$$

which after cancellation of terms is true by Lemma 2:

$$\frac{|G_{12}|}{|G_1|} \leq \frac{|G_{123}|}{|G_{13}|} \quad (24)$$

This completes the proof. $\blacksquare$

Next corollary follows immediately from Lemmas 5, 6.

Corollary 2. All groups of order pq , where p, q are distinct primes obey inequalities (9), (10).

C. Smallest Violating Group: S_4

Next we would like to find the smallest group which violates either (9) or (10). With the help of the above corollary we can eliminate a lot of groups of small order. First note that abelian groups cannot violate (9), (10). This allows us to eliminate groups of order p and p^2 , which are known to be abelian for any prime p . Additionally we can eliminate abelian-representable groups [12], i.e., groups whose corresponding joint entropies are known to be achieved by abelian groups. Among these are groups order 8. Together with Corollary 2, which eliminates groups of order pq for primes $p \neq q$, we conclude that up to order 24, violators of (9) or (10) may only be found among groups of order 12, 16, 18, 20 and 24. Having narrowed down the list of possible suspects, we verify using GAP that there exist no violators of order < 24 of either of the 2 inequalities. There does, in fact, exist a violator of order 24, as we show in the next proposition.

Proposition 1. The symmetric group S_4 of permutations over 4 elements violates (9).

Proof: Consider $G = S_4$, and

$$\begin{aligned} G_1 &= \langle (3, 4), (2, 4, 3) \rangle, & G_3 &= \langle (1, 2)(3, 4), (3, 4) \rangle \\ G_2 &= \langle (1, 3), (1, 3, 2) \rangle, & G_4 &= \langle (1, 3)(2, 4), (2, 4) \rangle \\ G_5 &= \langle (1, 4)(2, 3), (1, 3)(2, 4) \rangle \end{aligned}$$

with $|G_1| = 6$, $|G_2| = 6$, $|G_3| = 4$, $|G_4| = 4$, $|G_5| = 4$. Then

$$\begin{aligned} G_1 \cap G_2 &= \langle (2, 3) \rangle, & G_1 \cap G_3 &= \langle (3, 4) \rangle \\ G_2 \cap G_3 &= \langle (1, 2) \rangle, & G_1 \cap G_4 &= \langle (2, 4) \rangle \\ G_2 \cap G_4 &= \langle (1, 3) \rangle, & G_1 \cap G_5 &= \{1\} \end{aligned}$$

$$\begin{aligned} G_4 \cap G_5 &= \langle (1, 3)(2, 4) \rangle, & G_3 \cap G_4 \cap G_5 &= \{1\} \\ G_3 \cap G_5 &= \langle (1, 2)(3, 4) \rangle, & G_1 \cap G_2 \cap G_3 &= \{1\}. \end{aligned}$$

But for the trivial group, all the other intersection subgroups are of order 2. The right hand side of (9) yields

$$|G_{12}||G_{13}||G_{23}||G_{14}||G_{24}||G_{35}||G_{45}| = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 128$$

while the left hand side is

$$|G_2||G_3||G_{123}||G_{15}||G_{124}||G_4||G_{345}| = 6 \cdot 4 \cdot 1 \cdot 1 \cdot 1 \cdot 4 \cdot 1 = 96. \quad \blacksquare$$

IV. CONCLUSION

Random variables coming from finite groups have been studied before in order to provide an instance of violation of the Ingleton inequality in 4 random variables. This is of interest because Shannon-type inequalities together with the Ingleton inequality characterize linear rank inequalities in 4 random variables. In this article, we extended this study to 5 random variables, where for start we focused on 2 of the 24 additional inequalities that characterize linear rank inequalities. We showed that groups of order pq never violate either of these 2 inequalities, and that the symmetric group S_4 is in fact the smallest violator. Current and future work involve studying other inequalities for 5 random variables, and studying the subgroup structure of their violators.

V. ACKNOWLEDGMENTS

N. Markin was supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03. E. Thomas and F. Oggier were supported by Nanyang Technological University under Research Grant M58110049.

REFERENCES

- [1] W. Mao and B. Hassibi, "Violating the Ingleton Inequality with Finite Groups", *Allerton'09 Proceedings of the 47th annual Allerton conference on communication, control and computing*, Pages 1053-1060, 2009.
- [2] R. Yeung, "A First Course in Information Theory", in *Information Technology: Transmission, Processing, and Storage*, Springer (Kluwer Academic/Plenum Publishers), March 2002.
- [3] D. Hammer, A. Romashchenko, A. Shen, N. Vereshchagin, "Inequalities for Shannon Entropy and Kolmogorov Complexity", *Journal of Computer and System Sciences*, vol. 60, 2000.
- [4] A. Ingleton, "Representation of matroids," *Combinatorial Mathematics and its Applications*, 1971.
- [5] F. Matúš, "Conditional independences among four random variables I," *Combinatorics, Probability and Computing*, vol. 4, 1995.
- [6] R. Dougherty, C. Freiling and K. Zeger, "Linear rank inequalities on five or more variables", preprint, 2010, available at <http://arxiv.org/abs/0910.0284>
- [7] L. Guille, T.H. Chan and A. Grant, "The minimal set of Ingleton inequalities", *IEEE Transactions on Information Theory*, Pages 1849-1864, Volume.57, Issue.4, 2011.
- [8] T.H. Chan, "Aspects of Information Inequalities and its Applications", M.Phil Thesis, Dept. of Information Engineering, The Chinese University of Hong Kong, September 1998.
- [9] N. Boston and T.-T. Nan, "Large Violations of the Ingleton Inequality", *Allerton '12 Proceedings of the 47th annual Allerton conference on communication, control and computing*, 2012.
- [10] N. Boston, T.-T. Nan, "A Refinement of the Four-Atom Conjecture", *International Symposium on Network Coding(NetCod)*, 2013.
- [11] R. Stancu and F. Oggier, "Finite nilpotent and metacyclic groups never violate the Ingleton inequality", *International Symposium on Network Coding(NetCod)*, June 2012.
- [12] E.K. Thomas, N. Markin, F. Oggier, "On Abelian Group Representability of Finite Groups", preprint, <http://arxiv.org/abs/1212.1298>