ON GROUP VIOLATIONS OF INEQUALITIES
IN FIVE SUBGROUPS

NADYA MARKIN, ELDHO K. THOMAS AND FRÉDÉRIQUE OGGIER

Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University, Singapore

(Communicated by Camilla Hollanti)

Abstract. In this paper we use group theoretic tools to obtain random variables which violate linear rank inequalities, that is inequalities which always hold on ranks of subspaces. We consider ten of the 24 (non-Shannon type) generators of linear rank inequalities in five variables and look at them as group inequalities. We prove that for primes \( p, q \), groups of order \( pq \) always satisfy these ten group inequalities. We give partial results for groups of order \( p^2q \), and find that the symmetric group \( S_4 \) is the smallest group to yield violations for two among the ten group inequalities.

1. Introduction

For a collection \( X_1, \ldots, X_n \) of \( n \) discrete random variables with joint probability distribution \( P(x_1, \ldots, x_n) \),

\[
H(X_1, \ldots, X_n) = - \sum_{x_1} \cdots \sum_{x_n} P(x_1, \ldots, x_n) \log P(x_1, \ldots, x_n)
\]

is their joint (Shannon) entropy, where the logarithm is taken in base 2 if the entropy is expressed in bits, and \( P(x_1, \ldots, x_n) \log P(x_1, \ldots, x_n) \) is defined to be 0 if \( P(x_1, \ldots, x_n) = 0 \). For \( A \) a subset of \( \{1, \ldots, n\} \), we write \( H(X_A) \) for the joint entropy \( H(X_i, i \in A) \).

Let \( G \) be a finite group, and \( G_1, \ldots, G_n \) be subgroups of \( G \). Then

\[
G_A = \cap_{i \in A} G_i
\]

is a subgroup obtained by intersecting \( G_i, i \in A \). Let \( X \) be a random variable uniformly distributed over \( G \): \( P(X = g) = \frac{1}{|G|}, g \in G \). Then the random variable \( X_i = XG_i \) whose support is the \( [G : G_i] \) cosets of \( G_i \) in \( G \) satisfies \( P(X_i = gG_i) = \frac{|G_i|}{|G|} \) (see [1]) and

\[
P(X_i = gG_i, i \in A) = \frac{|\cap_{i \in A} G_i|}{|G|}.
\]

2010 Mathematics Subject Classification: Primary: 20D30; Secondary: 94A15.

Key words and phrases: Group inequalities, lattice of subgroups, linear inequalities, symmetric group.

This research was supported by Nanyang Technological University under Research Grant M58110049.
The entropy of the random variable $X_A = (X_i, \ i \in A)$, $X_i = XG_i$, is

$$H(X_A) = - \sum_{x_A} P(X_A = x_A) \log P(X_A = x_A)$$

$$= - \sum_{x_A, \ P(X_A = x_A) \neq 0} P(X_A = x_A) \log \frac{1}{P(X_A = x_A)}$$

$$= - \sum_{x_A, \ P(X_A = x_A) \neq 0} \frac{|G_A|}{|G|} \log \frac{|G|}{|G_A|}$$

$$= \log \frac{|G|}{|G_A|}$$

since the number of $x_A$ for which $P(X_A = x_A) \neq 0$ is $|G : G_A| = \frac{|G|}{|G_A|}$.

In what follows, we will only consider random variables $X_1, \ldots, X_n$ coming from a finite group $G$ and $n$ of its subgroups $G_1, \ldots, G_n$. Hence, to any information (in)quality (that is, (in)quality written as a function of joint Shannon entropies) expressed in terms of random variables $X_1, \ldots, X_n$ will correspond a group (in)quality which is a function of the subgroups $G_1, \ldots, G_n$, using $H(X_A) = \log \frac{|G|}{|G_A|}$. We can drop the logarithm from an inequality by exponentiating both sides. We will denote this correspondence from linear inequalities into the multiplicative group inequalities by $\mathcal{G}$.

For example:

- The conditional entropy $H(X_2|X_1) = H(X_1, X_2) - H(X_1)$ is expressed in terms of group as

  $$\mathcal{G}H(X_2|X_1) = \frac{|G|}{|G_{12}|} \frac{|G_1|}{|G|} = \frac{|G_1|}{|G_{12}|}.$$  

- The mutual information $I(X_1; X_2) = H(X_1) + H(X_2) - H(X_1, X_2)$ becomes

  $$\mathcal{G}I(X_1; X_2) = \frac{|G|}{|G_1|} \frac{|G_2|}{|G|} = \frac{|G_1|}{|G_1||G_2|}.$$  

- The conditional mutual information\(^1\) $I(X_1; X_2|X_3) = H(X_1|X_3) - H(X_1|X_2, X_3)$ is similarly

  $$\mathcal{G}I(X_1; X_2|X_3) = \frac{|G_3|}{|G_{13}|} \frac{|G_{123}|}{|G|}.$$  

Linear inequalities satisfied by any joint distribution of random variables, such as the non-negativity of the conditional mutual information

$$I(X_1; X_2|X_3) \geq 0,$$  

are called information inequalities. Similarly, linear inequalities satisfied by ranks of any vector subspace arrangement are called linear rank inequalities.

A vector space $V$ over a finite field $\mathbb{F}$, along with its subspaces $V_1, \ldots, V_n$ gives rise to random variables in the following fashion. Let $X$ be a uniform random

\(^1\)In this paper, we use as definition of the mutual information $I(X_1; X_2)$ that $I(X_1; X_1) = H(X_1) + H(X_2) - H(X_1, X_2)$ and similarly as definition of the conditional mutual information $I(X_1; X_2|X_3)$ that $I(X_1; X_2|X_3) = H(X_1|X_3) - H(X_1|X_2, X_3)$, though one often gives a definition of mutual information where the entropy is not written as such, namely $I(X_1; X_2) = \sum_{x_1} \sum_{x_2} p(x_1, x_2) \log \frac{p(x_1, x_2)}{p(x_1)p(x_2)}$. A similar expression exists for the conditional mutual information.
variable over the set of linear functions from $V$ to $\mathbb{F}$. Further let $X_i$ be the restriction $X_i|_{V_i}$ for each $i = 1, \ldots, n$. Each $X_i$ is a uniform random variable with $|F|^{\dim(V_i)}$ values, so $H(X_i|_{V_i}) = \dim(V_i) \log |F|$. This shows [5, Theorem 2] how information inequalities are a subset of linear rank inequalities. The converse is generally not true.

Consider the case of $n = 4$ random variables.

The Ingleton inequality [7]

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

always holds for ranks of subspaces, yet there are examples of random variables whose joint entropies violate the Ingleton inequality [11]. In the context of ranks of subspaces, $H(X_1)$ is understood as the rank of the subspace $X_1$, $H(X_1, X_2)$ as the rank of the span $\langle X_1, X_2 \rangle$, and $I(X_1; X_2)$ as the rank of $X_1 \cap X_2$, thus the fact that the mutual information $I(X_1; X_2)$ satisfies $I(X_1; X_2) = H(X_1) + H(X_2) - H(X_1, X_2)$ corresponds to the well-known formula that relates the rank of a span of two subspaces to that of their intersection.

The idea of looking at violations of the Ingleton inequality coming from groups was proposed in [9]. By a group violation, we mean a group $G$, with $n$ subgroups $G_1, \ldots, G_n$, such that the orders of the intersections of subgroups involved do not satisfy a given inequality. It was shown in [9] that the symmetric group $S_5$ and four of its subgroups $G_1, \ldots, G_4$ violate the group version of the Ingleton inequality

$$GI(X_1; X_2) \leq GI(X_1; X_2|X_3) GI(X_1; X_2|X_4) GI(X_3; X_4),$$
equivalently given by

$$|G_{12}||G_{13}||G_{14}||G_{23}||G_{24}| \leq |G_1||G_2||G_{34}||G_{123}||G_{124}|.$$ 

At the same time, it is also known [1] that abelian groups always satisfy the Ingleton inequality.

The Ingleton inequality plays a special role for $n = 4$ random variables. Together with the Shannon inequalities (a special case of information inequalities which are derived from the non-negativity of the conditional mutual information), the Ingleton inequality generates all linear rank inequalities in $n = 4$ random variables.

From an information theoretic view point, it is fundamental to understand the region $\Gamma_n^*$ formed by $(2^n - 1)$-dimensional vectors of the form $(H(X_A), A \subset \{1, \ldots, n\})$ where $A$ runs through all non-empty subsets of $\{1, \ldots, n\}$. Indeed, it has been shown that the capacity region of any arbitrary multi-source multi-sink acyclic network can be computed as a linear function of such vectors under linear constraints [6, 15]. But the problem of describing $\Gamma_n^*$ is notoriously difficult. The subset of $\Gamma_n^*$ consisting of entropy vectors obtained from linear subspaces (i.e those satisfying linear rank inequalities) on the other hand is too restricted, and only captures a small part of the region of interest. To further our understanding of the rest of $\Gamma_n^*$, we seek to find random variables violating linear rank inequalities. Using information theoretic tools only, this is not an easy task. Group theory provides a systematic way to address this question by considering the larger subset of $\mathbb{R}^{2^n - 1}$ consisting of elements of the form $(\frac{|G_i|}{|F|^{|A|}}, A \subset \{1, \ldots, n\})$ coming from groups [1]. From a practical point of view, the networks associated with this region may outperform those which are subject to linear constraints.

We therefore have the following hierarchy of the entropy region: entropies coming from subspaces $\subseteq$ entropies coming from groups $\subseteq$ entropies coming from all random variables. In case $n = 4$, the Ingleton inequality (along with Shannon-type
inequalities) completely characterises those entropy vectors coming from subspaces.

Consider now the case of $n = 5$ random variables. In [2], it was shown that 24 inequalities, together with the Shannon inequalities, and three Ingleton-type inequalities, generate all linear rank inequalities on five variables. In this paper, we are interested in looking at these inequalities from a group theoretic point of view. The motivation is the same as that of [9] for four random variables, namely: finding violators furthers our understanding of $\mathcal{I}_n^*$ beyond the subregion characterised by linear rank inequalities.

Among the inequalities of [2], the three Ingleton-type inequalities have already been studied in [10], where it was shown that a group does not violate the Ingleton inequality (1) if and only if it does not violate any of the three Ingleton-type inequalities in 5 random variables. We thus focus on the first 10 out of the 24 inequalities of [2] (since they share some commonalities, or more precisely, the same form of common information, see Lemma 1 below).

In Section 2, we prove some general properties about the group inequalities corresponding to the first 10 inequalities of [2], that we refer to as DFZ inequalities throughout the paper.

In Section 3, we prove that groups of order $pq$, where $p$ and $q$ are two primes, never violate any of the DFZ inequalities. By characterizing groups which never yield violations, we make the search for violators tractable by reducing it to smaller families of groups.

Partial results are given in Section 4, namely we show that groups $G$ of order $p^2q$ and subgroups $(G_1, G_2, G_3, G_4, G_5)$ do not violate the ten DFZ inequalities as long as $|G_1| = |G_2| = p$ does not hold. The case $|G_1| = |G_2| = p$ remains open, and we discuss why it is more difficult than the other ones.

Violators are discussed in Section 5, where we show that the smallest violator of two of the ten DFZ inequalities is the symmetric group $S_4$. We also show that it is not possible to find one group which simultaneously violate all the 10 DFZ inequalities.

Basic group theory is used in this paper, the interested reader may refer to [4] for a first introduction to group theory, to [12] for a course in group theory, and to [3] for general references about group theory.

2. Ten Group Inequalities

Recall that for $n = 5$ random variables, it was shown in [2] that 24 inequalities, together with the Shannon inequalities, and three Ingleton-type inequalities, generate all linear rank inequalities on 5 variables. The first 10 inequalities are

\begin{align}
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 | X_5) \\
&+ I(X_1; X_5), \\
I(X_1; X_2) &\leq I(X_1; X_2 | X_3) + I(X_1; X_3 | X_4) + I(X_1; X_4 | X_5) \\
&+ I(X_2; X_3), \\
I(X_1; X_2) &\leq I(X_1; X_3) + I(X_1; X_2 | X_4) + I(X_2; X_5 | X_3) + I(X_1; X_4 | X_3, X_5), \\
I(X_1; X_2) &\leq I(X_1; X_3) + I(X_1; X_2 | X_4, X_5) + I(X_2; X_4 | X_3) \\
&+ I(X_1; X_5 | X_3, X_4),
\end{align}

(2) (3) (4) (5)
Lemma 2. If inequalities (2)-(11).

Proof. We translate the above results on common information:

\[ I(X_1; X_2) \leq I(X_1; X_3) + I(X_2; X_4|X_3) + I(X_1; X_5|X_4) \]

(6)

\[ I(X_1; X_2) \leq +I(X_1; X_2|X_3, X_5) + I(X_2; X_3|X_4, X_5), \]

(7)

\[ I(X_1; X_2) \leq I(X_1; X_3) + I(X_2; X_4|X_5) + I(X_4; X_5|X_3) \]

(8)

\[ 2I(X_1; X_2) \leq I(X_1; X_3) + I(X_2; X_4|X_5) + I(X_1; X_2|X_3) \]

(9)

\[ 2I(X_1; X_2) \leq I(X_1; X_3) + I(X_2; X_4|X_5) + I(X_1; X_2|X_3) \]

(10)

\[ 2I(X_1; X_2) \leq I(X_1; X_3) + I(X_2; X_4|X_5) + I(X_1; X_2|X_3) \]

(11)

The following lemma reveals our motivation to look at the 10 DFZ inequalities.

Lemma 1 ([2]). Suppose there exists a random variable \( Z \), called common information, such that

\[ H(Z|X_1) = 0, \quad H(Z|X_2) = 0, \quad H(Z) = I(X_1; X_2), \]

then each of the 10 DFZ inequalities can be deduced from Shannon inequalities involving the random variables \( X_1, \ldots, X_5 \).

The other 14 inequalities are also deduced from Shannon inequalities through the concept of common information, but it takes different expressions.

Repeating the computations of the previous section, inequalities (2)-(11) have a corresponding group theoretic formulation, obtained via the correspondence \( G \):

\[ i_{1;2;3|G} := G I(X_1; X_2, X_3) = \frac{|G_{123}||G|}{|G_{12}||G_{23}|}, \]

\[ i_{1,2;3,4|G} := G I(X_1, X_2; X_3, X_4) = \frac{|G_{1234}||G|}{|G_{12}||G_{34}|}, \]

\[ i_{1;2|3} := G I(X_1; X_2|X_3) = \frac{|G_{123}||G_3|}{|G_{13}||G_{23}|}, \]

\[ i_{1;2|3,4} := G I(X_1; X_2|X_3, X_4) = \frac{|G_{1234}||G_{34}|}{|G_{134}||G_{234}|} \]

yielding accordingly 10 groups inequalities, which we will freely refer to as group inequalities (2)-(11).

The notion of common information is also expressible in the language of groups:

**Lemma 2.** If \( G_1G_2 \) is a subgroup of \( G \), then the group inequalities (2)-(11) hold.

**Proof.** We translate the above results on common information:

\[ H(Z|X_1) = 0 \Leftrightarrow \log \frac{|G|}{|G_1|} = \log \frac{|G|}{|G_Z \cap G_1|} \Leftrightarrow G_1 < G_Z, \]
similarly $H(Z|X_2) = 0 \iff G_2 < G_Z$ and

$$H(Z) = I(X_1; X_2) \iff \log \frac{|G|}{|G_Z|} = \log \frac{|G|}{|G_1|} + \log \frac{|G|}{|G_2|} - \log \frac{|G|}{|G_12|}$$

$$\iff |G_Z| = \frac{|G_1||G_2|}{|G_12|}.$$ 

If $G_1G_2$ is a subgroup of $G$, take $G_Z = G_1G_2$, then

$$|G_1G_2| = \frac{|G_1||G_2|}{|G_12|}, \quad G_1 < G_1G_2, \quad G_2 < G_1G_2$$

which shows the existence of common information and concludes the proof. □

**Corollary 1.** The above 10 DFZ inequalities hold in the following cases:

1. $G_1 < G_2$, or $G_2 < G_1$.
2. $G_1$ or $G_2$ is normal in $G$.
3. $G$ is abelian.

We will use the following lemma and corollary to prove many inequalities.

**Lemma 3.** Let $G$ be a finite group with $n$ subgroups $G_1, \ldots, G_n$. For any choice of subsets $A_1, A_2, A_3$ of $\{1, \ldots, n\}$

$$|G_{A_1\cup A_2}| |G_{A_1\cup A_3}| \leq |G_{A_1}| |G_{A_1\cup A_2\cup A_3}| \leq |G_{A_1}| |G_{A_2\cup A_3}|$$

is always satisfied.

Moreover, if one of $G_{A_1\cup A_2}, G_{A_1\cup A_3}$ is normal, then

$$\frac{|G_{A_1\cup A_2}| |G_{A_1\cup A_3}|}{|G_{A_1\cup A_2\cup A_3}|} \text{ divides } |G_{A_1}|.$$

**Proof.** We use the fact that the subset $G_{A_1\cup A_2}G_{A_1\cup A_3} \leq G_{A_1}$ has cardinality

$$\frac{|G_{A_1\cup A_2}| |G_{A_1\cup A_3}|}{|G_{A_1\cup A_2\cup A_3}|}.$$ 

Moreover when one of $G_{A_1\cup A_2}, G_{A_1\cup A_3}$ is normal, then the subset $G_{A_1\cup A_2}G_{A_1\cup A_3}$ is actually a subgroup of $G_{A_1}$, hence its size divides $|G_{A_1}|$. □

Relating the lemma above to information quantities $i_{a;b|c} = \frac{|G_{ab}| |G_c|}{|G_{ac}| |G_{bc}|}$ and $i_{a;b|c,d} = \frac{|G_{abcd}| |G_{ad}|}{|G_{acd}| |G_{bc}|}$ gives the following immediate corollary.

**Corollary 2.** Consider subgroups $G_a, G_b, G_c, G_d \leq G$ with corresponding random variables $X_a, X_b, X_c, X_d$. The following bounds hold:

$$1 \leq i_{a;b|c} \text{ and } 1 \leq i_{a;b|c,d}.$$ 

Moreover, if either $G_{ac} \leq G_c$ or $G_{bc} \leq G_c$ then $i_{a;b|c}$ and $i_{a;b|c,d}$ are both integers.

**Proof.** Recall that $i_{a;b|c} = \frac{|G_{acb}| |G_c|}{|G_{ac}| |G_{bc}|}$ and $i_{a;b|c,d} = \frac{|G_{abcd}| |G_{cd}|}{|G_{acd}| |G_{bc}|}$. We apply the lemma above for subsets $A_1 = \{c\}, A_2 = \{a\}, A_3 = \{b\}$ to show the first inequality. We apply the lemma above for subsets $A_1 = \{cd\}, A_2 = \{a\}, A_3 = \{b\}$ to show the second inequality. The last statement is similarly a direct consequence of the lemma. □

Next we show how uniqueness of a Sylow $q$-subgroup imposes constraints on quantities $i_{a;b|c}$. We will use the valuation $v_q$ at a prime $q$. For integers $u, v$, let $q^u$ and $q^v$ be the powers of $q$ that appear in the respective prime factorization of $u$ and $v$. The valuation $v_q(u - v)$ is by definition $e_u - e_v$. 

**Advances in Mathematics of Communications** Volume 10, No. 4 (2016), 871-893
\textbf{Lemma 4.} Let $G$ be a group whose Sylow $q$-subgroup is normal and abelian. For any two subgroups $A, B \leq G$, let $AB = \{ab : a \in A, b \in B\}$ denote the set-product of $A, B$. Then
\[ v_q(|G|) \geq v_q(|AB|). \]

\textit{Proof.} Let $G_q$ (resp. $A_q, B_q$, $(A \cap B)_q$) denote the Sylow $q$-subgroup of $G$ (resp. $A, B, A \cap B$). Then we have
\[
 v_q(|AB|) = v_q(|A|) + v_q(|B|) - v_q(|A \cap B|) =
 v_q(|A_q|) + v_q(|B_q|) - v_q((A \cap B)_q) = v_q(|A_qB_q|) \leq v_q(|G_q|).
\]
To see the last inequality note first that $A_q$ and $B_q$ are both contained in $G_q$, since $G_q$ is normal (or equivalently unique). Moreover, since $G_q$ is by assumption abelian, $A_qB_q$ in fact forms a subgroup, not just a subset of $G_q$. Hence we know that $|A_qB_q|$ divides $|G_q|$. \hfill \Box

As a corollary we get the following proposition.

\textbf{Proposition 1.} Let $G$ be a group whose Sylow $q$-subgroup is normal and abelian. Let $G_a, G_b, G_c$ be arbitrary subgroups of $G$. Then $v_q(i_{a,b,c}) \geq 0$.

\textit{Proof.} Apply previous Lemma with $G = G_c$, $A = G_{ac}, B = G_{bc}$. Then
\[
 v_q(i_{a,b,c}) = v_q\left[\frac{G_{abc}}{|G_{ac}||G_{bc}|}\right] = v_q(|G_c|) - v_q(|G_{ac}G_{bc}|) \geq 0.
\] \hfill \Box

\textbf{Remark 1.} The fact that there is only one (normal) Sylow $q$-subgroup restricts powers of $q$ in expression $i_{a,b,c}$ to positive ones. This eventually allows us to prove our results for groups of order $pq$ and $p^2q$ in the following two sections.

3. Groups of order $pq$

In this section we prove that information inequalities (2)-(11) hold for groups of order $pq$

First we make a few observations about these groups. The property described in the lemma below was used to prove inequalities (2)-(3) in [10].

\textbf{Lemma 5.} A group $G$ has the property that all its distinct proper subgroups have trivial intersection if and only if $|G| = pq$, where $p, q$ are either 1 or prime, not necessarily distinct.

\textit{Proof.} Suppose $|G| = pq$ and consider two proper distinct non-trivial subgroups $A, B$ of $G$. If $|A| = p$ and $|B| = q$ for $p \neq q$, or vice-versa, they necessarily intersect trivially. If $|A| = |B| = p$ (or $q$ if $p = q$), then any non-trivial element of $A \cap B$ generates all of $A$ and all of $B$, as they are of prime order - a contradiction since $A, B$ are distinct.

Conversely, assume the property that all proper subgroups of $G$ have trivial intersection. We will show that the order $n$ of $G$ is $pq$.

Case 1: $G$ is equal to its Sylow $p$-subgroup. Then $|G| = p^t$ and it is a standard exercise using central series of $G$ to show that $G$ contains a subgroup $p^h$ for each $1 \leq k \leq t$. It follows that if $t > 2$, then $G$ contains a (proper) subgroup of order $p^2$, which in turn has a subgroup of order $p$. These two subgroups have non-trivial intersection, contradicting our assumption on $G$. We conclude $t \leq 2$.

Case 2: All Sylow subgroups are proper.
We show that all Sylow subgroups are cyclic and hence \( n \) is a product of distinct primes. Consider a Sylow \( p \)-subgroup \( S_p \) of order \( p^t \). It suffices to show that \( t = 1 \). Suppose, to the contrary, that \( t \geq 2 \). Then by Cauchy theorem, \( S_p \) contains a cyclic subgroup \( C_p \) of order \( p \), so \( S_p \) and \( C_p \) are two proper subgroups which intersect non-trivially - a contradiction.

Next we show that the number of divisors of \( n \) is at most \( 2 \). Suppose to the contrary, that the order \( n \) of \( G \) is divisible by at least three primes \( p, q, r \).

Then \( pq \) is a Hall divisor of \( n \) - that is \( pq \mid n, \gcd(pq, \frac{n}{pq}) = 1 \). Hence there exists a Hall-\( pq \) subgroup - a (proper) subgroup of order \( pq \). But it will then intersect non-trivially with a Sylow \( p \)-subgroup - a contradiction.

Next we show that (2)-(11) hold for groups of order \( pq \). The case \( |G| = p^2 \) is covered by abelian groups, which are known not to violate DFZ inequalities by Corollary 1. In what follows we hence assume that \( |G| = pq \), with primes \( p < q \).

Normality (equivalently, uniqueness) of Sylow \( q \)-subgroup plays an important role in establishing inequalities over the next two sections.

**Lemma 6.** If \( |G| = pq \), \( p < q \), then \( G \) contains exactly one Sylow \( q \)-subgroup. Equivalently if a subgroup \( H \leq G \) has order \( q \), then it is necessarily normal.

**Proof.** This is an elementary exercise in group theory. Sylow’s theorems tell that the number \( n_q \) of Sylow \( q \)-subgroup divides \( pq \) and \( n_q = 1 + kq \) for some \( k \) a positive integer, and also \( n_q \mid |G| = pq \). Since \( p < q \), the only choice left is \( n_q = 1 \). The second claim follows from the fact that Sylow subgroups are conjugate of each other.

**Corollary 3.** Let \( |G| = pq \), with primes \( p < q \). If \( G_1, G_2 \leq G \) are subgroups of \( G \), such that the set \( G_1G_2 = \{g_1g_2 : g_1 \in G_1, g_2 \in G_2 \} \) does not form a subgroup, then \( G_1, G_2 \) are distinct subgroups each of order \( p \).

**Proof.** If the subgroups are not distinct, we have \( G_1G_2 = G_1 \) is a subgroup. If one of \( G_1, G_2 \) is normal, then the set \( G_1G_2 \) forms a subgroup. But a subgroup of order other than \( p \) is necessarily normal and the result follows.

Now we set out to prove inequalities (2)-(11) for groups of order \( pq \). All these inequalities comprise mutual information terms, of the general form

\[
I(X_a; X_b), \quad I(X_a; X_b|X_c)
\]

for \( a, b, c \) some indices or subsets in \( \{1, 2, 3, 4, 5\} \). In group form, we have

\[
i_{a,b|G} = G \frac{I(X_a; X_b)}{|G_a||G_b|},
\]

\[
i_{a,b|c} = G \frac{I(X_a; X_b|X_c)}{|G_{ac}||G_{bc}|}.
\]

The next proposition shows how normality of the Sylow \( q \)-subgroup (guaranteed by Lemma 6) restricts information quantities \( i_{a,b|c} \).

**Proposition 2.** Let \( G \) be a group of order \( pq \), for primes \( p < q \), so the Sylow \( q \)-subgroup is unique. Each quantity \( i_{a,b|c}, i_{a,b|G}, i_{a,b|c,d} \) is \( \geq 1 \) and takes values among \( \{1, p, \frac{p}{q}, q, pq\} \).

**Proof.** Let us make the argument in the case of the quantity \( i_{a,b|c} = \frac{|G_{abc}|G_c}{|G_{ac}||G_{bc}|} \), which is the same as \( \frac{|G_c|}{|G_{ac}||G_{bc}|} \). Since \( G_{ac}G_{bc} \) is a subset of \( G_c \), \( \frac{|G_{abc}|G_c}{|G_{ac}||G_{bc}|} \geq 1 \). Since the
Sylow $q$-subgroup is unique (equivalently, normal), by Proposition 1, $v_q(i_{a;b;c}) \geq 0$, so the powers of $q$ occurring in $i_{a;b;c}$ can be only 0, 1. Now since $G_{ac} \leq G_c$, $G_{bc} \leq G_c$, the powers of $p$ are restricted to $-1, 0, 1$, and

$$\frac{|G_{abc}| |G_c|}{|G_{ac}||G_{bc}|} \in p^{-1,0,1}q^{0,1}.$$ 

The case $\frac{1}{p}$ cannot happen since $i \geq 1$.

The next two quantities follow as special cases.

In case of the second quantity $i_{a;b;G} = \frac{|G_{abc}| |G_c|}{|G_{ac}||G_{bc}|}$, we use $c = \emptyset$, i.e. $G_c = G$. In case of the third quantity $i_{a;b;c,d} = \frac{|G_{abc}| |G_{cd}|}{|G_{ac}||G_{bc}||G_{cd}|}$, we just substitute $G_c$ with $G_{cd}$ and the same argument holds.

By abuse of notation write $q \mid i_{a;b;c}$ when $v_q(i_{a;b;c}) > 0$, i.e., the quantity $i_{a;b;c}$ takes value among $\{q/p, q, pq\}$ (even if some of these are not integers). Conversely we will write $q \nmid i_{a;b;c}$, to indicate $i_{a;b;c}$ takes value among $\{1, p\}$.

Finally we make one small observation, which we will use a lot, thus it deserves to be stated as the following lemma.

**Lemma 7.** Let $i$ denote one of the information quantities $i_{a;b;c}, i_{a;b;G}$ or $i_{a;b;c,d}$.

Suppose $q \nmid i$. Then we have

$$q \mid |G_c| \implies q \mid |G_a||G_b|$$

or alternatively

$$q \nmid |G_a||G_b| \implies q \nmid |G_c|.$$ 

**Proof.** Consider the first case $i = \frac{|G_{abc}| |G_c|}{|G_{ac}||G_{bc}|}$. By assumption $q \nmid |G_{abc}| |G_c| |G_{ac}||G_{bc}|$. Rewrite $\frac{|G_{abc}| |G_c|}{|G_{ac}||G_{bc}|}$ as $\frac{|G_c|}{|G_{ac}||G_{bc}|}$. Depending on whether $G_{ac}G_{bc}$ forms a subgroup, this may or may not be an integer. However, if $q \mid |G_c|$, yet $q \nmid |G_{abc}| |G_c| |G_{ac}||G_{bc}|$, then necessarily $q \mid |G_{ac}G_{bc}|$, so a fortiori $q \mid |G_cG_{bc}|$. But then $q \mid |G_a|$ or $q \mid |G_b|$, so $q \mid |G_a||G_b|$. Taking the contrapositive gives the other implication $q \nmid |G_a||G_b|$ $\implies$ $q \nmid |G_c|$. The cases $i_{a;b;G}$ or $i_{a;b;c,d}$ follow, as discussed in the previous lemma, as special cases of the first case. 

We are now ready to prove the main proposition of this section.

**Proposition 3.** Let $G$ be a group of order $pq$, for primes $p < q$, so the Sylow $q$-subgroup is unique.

Then (2)-(11) hold for $G$.

**Proof.** We start by proving in detail inequality (4), which in its unsimplified group form is

$$\frac{|G_{12}| |G|}{|G_1||G_2|} \leq \frac{|G_{13}| |G| |G_{124}| |G_4|}{|G_1||G_3||G_4|} \cdot \frac{|G_{253}| |G_3|}{|G_{23}| |G_{53}|} \cdot \frac{|G_{14(35)}| |G_{35}|}{|G_{14}| |G_{35}|}$$

$$=: \frac{|G_{13}| |G|}{|G_1||G_3|}I_1 \cdot I_2 \cdot I_3$$

where we have labeled the last three factors as $I_1 = i_{1;2;4}$, $I_2 = i_{2;5;3}$ and $I_3 = i_{1;4;3.5}$.

We first prove the following claim about this inequality. Identical reasoning applies to other inequalities and we will simply refer to this claim when needing to invoke it.

Recall that by abuse of notation write $q \mid RHS$ to mean that one of the factors on the RHS takes value among $q/p, q, pq$ (even if some of these are not integers).
Claim 1. It suffices to show that \( q \mid \text{RHS} \).

It has been shown in Lemma 2 that when \( G_1G_2 \) is a subgroup of \( G \) such inequalities hold. Hence we only need to consider the case when the set \( G_1G_2 \) is not a subgroup, which by Corollary 3 occurs when \( G_1, G_2 \) are distinct, each of order \( p \), so we have \( |G_1| = |G_2| = \frac{q}{p} \).

The LHS is \( \left( \frac{|G_{12}|}{|G_1||G_2|} \right) = \frac{q}{p} \), while each of the factors on the right hand side takes values among \( \{1, p, q/p, q, pq\} \). Clearly, if \( q \) divides one of the factors on the RHS, the inequality holds since each of the (other) factors is \( \geq 1 \). This proves the claim.

Claim 2. We show that \( q \mid \text{RHS} \).

Suppose for the sake of contradiction that \( q \not\mid \left( \frac{|G_{12}|}{|G_1||G_2|} \right) I_1 \cdot I_2 \cdot I_3 \).

Recall, that throughout we are assuming \( G_1, G_2 \) are distinct groups of order \( p \). So in particular \( q \not\mid |G_1||G_2| \). We apply Lemma 7 successively to factors of the RHS to obtain a contradiction. More precisely:

By Lemma 7, \( \left\{ q \not\mid \left( \frac{|G_{12}|}{|G_1||G_2|} \right) I_1 \cdot I_2 \cdot I_3 \right\} \implies q \not\mid |G_1||G_3| \). But \( |G_1| = p \), hence \( q \not\mid |G_3| \).

By Lemma 7 \( \left\{ q \not\mid I_1 = \left( \frac{|G_{12}|}{|G_1||G_2|} \right) q \not\mid |G_2||G_1| \right\} \implies q \not\mid |G_4| \).

Next use the fact that \( q \not\mid |G_1| \) and \( q \not\mid |G_4| \) which we just showed. By Lemma 7, \( \left\{ q \not\mid I_3 = \left( \frac{|G_{12}|}{|G_1||G_2|} \right) q \not\mid |G_1||G_4| \right\} \implies q \not\mid |G_35| \). But recall we assumed that \( q \not\mid |G_5| \). Hence \( q \not\mid |G_5| \).

Next, apply Lemma 7 to \( I_2 = \left( \frac{|G_{23}|}{|G_3||G_5|} \right) \) together with \( q \not\mid |G_2||G_5| \) to conclude that \( q \not\mid |G_3| \). But then \( \left\{ q \not\mid |G_1|, q \not\mid |G_3| \right\} \implies q \not\mid \left( \frac{|G_{13}|}{|G_1||G_3|} \right) \) by Lemma 7. So we arrive that \( q \not\mid I_1 \mid \text{RHS} \), contradiction.

Hence we showed that \( q \mid \text{RHS} \), so by claim 1 the inequality is satisfied.

We proceed in the same fashion for other inequalities. Each of these inequalities has the form

\[
\frac{|G_{12}|}{|G_1||G_2|} \leq \frac{|\text{subgroup}||G|}{|\text{subgroup}|} I_1 \cdot I_2 \cdot I_3
\]

where in each case \( I_1, I_2 \) and \( I_3 \) will denote some information quantities on subgroups \( G_1, G_2, G_3, G_4, G_5 \). As before it suffices to show that one of the factors on the RHS takes value among \( \{1, p, q/p, q, pq\} \).

Inequality (2).

\[
\frac{|G_{12}|}{|G_1||G_2|} \leq \frac{|G_{12}|}{|G_1||G_2|} \cdot \frac{|G_{12}|}{|G_1||G_2|} = \frac{|G_{12}|}{|G_1||G_2|} I_1 \cdot I_2 \cdot I_3
\]

with the last three factors now labeled as \( I_1, I_2, I_3 \).

We have \( \left\{ q \not\mid \left( \frac{|G_{12}|}{|G_1||G_2|} \right), q \not\mid |G_1| \right\} \implies q \not\mid |G_5| \), by Lemma 7.

Suppose \( q \not\mid I_1, I_2, I_3 \). Apply successively Lemma 7 to get a contradiction: \( q \not\mid I, q \not\mid |G_1||G_2| \implies q \not\mid |G_3|, q \not\mid I_2, q \not\mid |G_1||G_2| \) thus \( q \not\mid |G_4| \) and Lemma 7 applies to \( I_3 \) yields \( q \not\mid |G_5| \), a contradiction.
Inequality (3).

\[
\frac{|G_{12}|}{|G_1||G_2|} \leq \frac{|G_{25}|}{|G_2||G_5|} \left( \frac{|G_{123}|}{|G_2||G_{25}|} \right) \left( \frac{|G_{124}|}{|G_4||G_{234}|} \right) \left( \frac{|G_{125}|}{|G_5||G_{245}|} \right)
\]

=: \frac{|G_{25}|}{|G_2||G_5|} I_1 \cdot I_2 \cdot I_3

with the last three factors now labeled as \( I_1, I_2, I_3 \).

Suppose \( q \nmid \text{RHS} \). \( \{ q \nmid \frac{|G_{25}|}{|G_2||G_5|}, q \nmid |G_2| \} \implies q \mid |G_5| \), by Lemma 7.

Apply Lemma 7 successively to factors \( I_1, I_2, I_3 \), to get \( q \mid |G_5| \), a contradiction.

Inequality (5).

\[
\frac{|G_{12}|}{|G_1||G_2|} \leq \frac{|G_{13}|}{|G_1||G_3|} \left( \frac{|G_{1234}|}{|G_{234}|} \right) \left( \frac{|G_{125}|}{|G_5||G_{25}|} \right) \left( \frac{|G_{135}|}{|G_3||G_{235}|} \right) \left( \frac{|G_{235}|}{|G_{25}|} \right) \left( \frac{|G_{245}|}{|G_{234}|} \right) \left( \frac{|G_{2345}|}{|G_{245}|} \right)
\]

=: \frac{|G_{13}|}{|G_1||G_3|} I_1 \cdot I_2 \cdot I_3 \cdot I_4

with the last three factors now labeled as \( I_1, I_2, I_3, I_4 \).

Suppose \( q \nmid \text{RHS} \). \( \{ q \nmid \frac{|G_{13}|}{|G_1||G_3|}, q \nmid |G_1| \} \implies q \mid |G_3| \), by Lemma 7.

Suppose \( q \nmid |G_3| \), \( q \mid |G_1| \), by Lemma 7.

We already concluded \( q \mid |G_5| \), so together with \( q \mid |G_4| \), we have \( q \mid |G_5| \).

But \( q \mid |G_3| \), \( q \mid |G_4| \), implies \( q \mid |G_3| \), a contradiction.

Inequality (6).

\[
\frac{|G_{12}|}{|G_1||G_2|} \leq \frac{|G_{13}|}{|G_1||G_3|} \left( \frac{|G_{12345}|}{|G_{2345}|} \right) \left( \frac{|G_{1235}|}{|G_{154}|} \right) \left( \frac{|G_{125}|}{|G_5||G_{25}|} \right) \left( \frac{|G_{135}|}{|G_3||G_{235}|} \right) \left( \frac{|G_{235}|}{|G_3||G_{235}|} \right) \left( \frac{|G_{245}|}{|G_{234}|} \right) \left( \frac{|G_{2345}|}{|G_{245}|} \right)
\]

=: \frac{|G_{13}|}{|G_1||G_3|} I_1 \cdot I_2 \cdot I_3 \cdot I_4

with the last four factors now labeled as \( I_1, I_2, I_3, I_4 \).

Suppose \( q \nmid \text{RHS} \). \( \{ q \nmid \frac{|G_{13}|}{|G_1||G_3|}, q \nmid |G_1| \} \implies q \mid |G_3| \), by Lemma 7.

Then \( q \mid |G_3| \), \( q \mid |G_4| \), and on \( I_2 \) gives \( q \mid |G_4| \), a contradiction.

Inequality (7).

\[
\frac{|G_{12}|}{|G_1||G_2|} \leq \frac{|G_{13}|}{|G_1||G_3|} \left( \frac{|G_{12345}|}{|G_{2345}|} \right) \left( \frac{|G_{12354}|}{|G_{154}|} \right) \left( \frac{|G_{125}|}{|G_5||G_{25}|} \right) \left( \frac{|G_{135}|}{|G_3||G_{235}|} \right) \left( \frac{|G_{235}|}{|G_3||G_{235}|} \right) \left( \frac{|G_{245}|}{|G_{234}|} \right) \left( \frac{|G_{2345}|}{|G_{245}|} \right)
\]

=: \frac{|G_{13}|}{|G_1||G_3|} I_1 \cdot I_2 \cdot I_3 \cdot I_4

with the last four factors now labeled as \( I_1, I_2, I_3, I_4 \).

Suppose \( q \nmid \text{RHS} \). \( \{ q \nmid \frac{|G_{13}|}{|G_1||G_3|}, q \nmid |G_1| \} \implies q \mid |G_3| \), by Lemma 7.

Then \( q \mid |G_3| \), \( q \mid |G_4| \), and on \( I_2 \) gives \( q \mid |G_4| \), a contradiction.

Applying Lemma 7 to factor \( I_1 \), then \( I_2 \), we get a contradiction.
Hence $q$ with the last four factors now labeled as $I_1, I_2, I_3, I_4$.

Next suppose $q \nmid \text{RHS}$.

Claim 3. In order to prove the inequality, it suffices to show that the power of $q$ dividing $I_1 \cdot I_2 \cdot I_3 \cdot I_4 \cdot I_5$ is at least 2.

The LHS is $(\frac{|G_{12}|}{|G_{12}|/|G_{12}|}) = (\frac{2}{p})^2$, while each of the factors on the right hand side takes values among $\{1, p, q/p, q, pq\}$. Clearly if at least two of them are among $q/p, q, pq$, the inequality holds for each $I_1, I_2, I_3, I_4, I_5 \geq 1$ by Proposition 2. This proves the claim.

Next we show that the condition of the claim is indeed satisfied.

Claim 4. The power of $q$ dividing $I_1 \cdot I_2 \cdot I_3 \cdot I_4 \cdot I_5$ is at least 2.

Recall that $\frac{|G_{12}|}{|G_{12}|/|G_{12}|}$ takes values $\{1, p\}$ only when $q \mid |G_a||G_b|$, by Proposition 2.

Hence $q \mid I_1 \cdot I_3 \cdot I_4$, so if $q \nmid I_1$, then it must divide either $I_3$ or $I_4$. Next suppose $q \mid I_2$. 

Hence $q \mid I_2 \cdot I_5 \cdot I_4$, so if $q$ does not divide $I_2$, then it must divide either $I_5$ or $I_4$. The problem now is - what if $I_4$ is used to “make up for” $q \nmid I_1$ and $q \nmid I_2$ simultaneously?

So suppose $q \nmid I_1, q \mid I_2, q \mid I_4$. We must demonstrate that $q$ divides at least one other factor.

$$\frac{|G_{12}|}{|G_{12}|/|G_{12}|} \leq \left(\frac{|G_{12}|}{|G_{12}|/|G_{12}|}\right) \cdot \left(\frac{|G_{534}|}{|G_{534}|/|G_{534}|}\right) \cdot \left(\frac{|G_{123}|}{|G_{123}|/|G_{123}|}\right) \cdot \left(\frac{|G_{124}|}{|G_{124}|/|G_{124}|}\right) \cdot \left(\frac{|G_{125}|}{|G_{125}|/|G_{125}|}\right)$$

$\Rightarrow I_1 \cdot I_2 \cdot I_3 \cdot I_4 \cdot I_5$
We have $q \nmid I_3 \implies q \mid |G_3|$, and $q \mid I_4 \implies q \mid |G_4|$, so together $q \nmid |G_{34}|$.
Then $q \mid |G_{34}|$, $q \nmid I_2 \implies q \mid |G_5| \implies q \mid I_5$ and we found another term, as desired.

**Inequality (10).**

\[
\frac{|G_{12}| |G|}{|G_1||G_2|} \leq \left( \frac{|G_{13}| |G|}{|G_1||G_3|} \right) \left( \frac{|G_{14}| |G|}{|G_1||G_4|} \right) \left( \frac{|G_{15}| |G|}{|G_1||G_5|} \right) \left( \frac{|G_{124}| |G|}{|G_{124}||G_{24}|} \right) \left( \frac{|G_{125}| |G|}{|G_{125}||G_{25}|} \right) \left( \frac{|G_{145}| |G|}{|G_{145}||G_{45}|} \right)
\]

with the factors now labeled as $I_1, I_2, I_3, I_4, I_5$.

Suppose $q \nmid I_1$, then $q \mid |G_3|$.
$q \mid |G_3| \implies q \mid I_5$ or $q \mid |G_{45}|$.
$q \mid |G_{45}| \implies q \mid |G_5| \implies q \mid I_4$.
$q \mid |G_4| \implies q \mid |G_4| \implies q \mid I_3$.
We conclude $q \nmid I_1 \implies q \mid I_5$ or $(q \mid I_4$ and $q \nmid I_3)$.
Suppose $q \nmid I_2$, then $q \mid |G_4||G_5| \implies q \mid I_3 \cdot I_4$.
$q \nmid I_1$ and $q \nmid I_2$ results in at least two factors of $I_3, I_4, I_5$ which $q$ divides, as desired.

**Inequality (11).**

\[
\left( \frac{|G_{12}| |G|}{|G_1||G_2|} \right) \left( \frac{|G_{12}| |G|}{|G_1||G_2|} \right) \leq \left( \frac{|G_{13}| |G|}{|G_3||G_4|} \right) \left( \frac{|G_{15}| |G|}{|G_3||G_5|} \right) \left( \frac{|G_{123}| |G_3|}{|G_1||G_3|} \right) \left( \frac{|G_{124}| |G_4|}{|G_1||G_4|} \right) \left( \frac{|G_{245}| |G_5|}{|G_4||G_5|} \right) \left( \frac{|G_{123}| |G_3|}{|G_1||G_3|} \right) \left( \frac{|G_{124}| |G_4|}{|G_1||G_4|} \right) \left( \frac{|G_{245}| |G_5|}{|G_4||G_5|} \right) \left( \frac{|G_{123}| |G_3|}{|G_1||G_3|} \right) \left( \frac{|G_{124}| |G_4|}{|G_1||G_4|} \right) \left( \frac{|G_{245}| |G_5|}{|G_4||G_5|} \right)
\]

with the factors now labeled as $I_1, I_2, I_3, I_4, I_5, I_6$.

Suppose $q \nmid I_1$, then $q \mid |G_3||G_4|$.
Suppose $q \nmid I_2$, then $q \mid |G_5|$.
$q \mid |G_5| \implies$ either $q \mid I_5$ or $q \mid |G_4|$. $q \mid |G_4| \implies q \mid I_4$.
We summarize: $q \nmid I_2 \implies q \mid I_4 \cdot I_5$.
Suppose $q \nmid I_1$ and $q \nmid I_2$. We want to show that $I_4$ cannot be the only factor divisible by $q$. Suppose then $q \nmid I_1$ and $q \nmid I_2$. We show that $q$ divides another factor. For the sake of contradiction, suppose $q$ only divides $I_4$.
$q \nmid I_2 \implies q \mid |G_5|$. $q \mid I_4 \implies q \mid |G_4|$. $q \nmid I_3 \implies q \mid |G_3|$. $q \mid I_6 \implies q \mid |G_{45}|$. $q \mid |G_{45}|, q \mid |G_4| \implies q \mid |G_5|$, a contradiction to $q \nmid I_2$. This completes the proof of the proposition.

4. **Groups of order $p^2q$**

Next we consider groups of order $p^2q$, $p,q$ two distinct primes. We are interested in seeing how far the techniques developed for the case $pq$ can be extended for the case $p^2q$. Unfortunately we cannot derive a complete generalization of Proposition 3 and show that DFZ inequalities necessarily hold for these groups. However, we are able to use similar reasoning to derive partial results, which can be used to reduce computation when looking for violators of DFZ inequalities. The case $|G_1| = |G_2| = p$ remains open.

The following lemma is an exercise in elementary group theory.
Lemma 8. Let $G$ be a group of order $p^2q$. Then $G$ has at least one normal Sylow subgroup.

Proof. Case $q < p$. We show that the Sylow $p$-subgroup is normal. Sylow theorems give us the following constraints on the number $n_p$ of Sylow $p$-subgroups:

- $n_p = 1 + kp$, $k \geq 0$,
- $n_p | p^2q$.

Together we have $n_p | q$. But as by assumption $q < p$, the first constraint rules out the case that $n_p = q$. We conclude that $n_p = 1$ so the Sylow $p$-subgroup is unique. Equivalently, Sylow $p$-subgroup is normal since Sylow subgroups are conjugates of one another.

Case $p < q$. We have $n_q = 1 + kq$ divides $p^2$ and $n_p = 1 + lp$ divides $q$, $k, l \geq 0$, thus $n_q \in \{1, p, p^2\}$.

- Case $n_q = 1$. Then the Sylow $q$ subgroup is unique, and we are done.
- Case $n_q = p$ cannot occur for $1 + kq = p$ will contradict $p < q$.
- Case $n_q = p^2$. We show that this forces $n_p = 1$, i.e. the Sylow $p$-subgroup to be unique. Note that the number of elements of order $q$ is $(q - 1)p^2$, thus the number of elements of order $p^t$, $t = 0, 1, 2$, is $p^2q - (q - 1)p^2 = p^2$. But that is precisely the order of any Sylow $p$-subgroup. Therefore all elements of order $p$ are included in a single Sylow $p$-subgroup. Hence there is a unique Sylow $p$-subgroup and we are done.

We have concluded that $G$ has at least one unique Sylow subgroup - and it can correspond to either of the prime divisors of $G$.

As per Remark 1, we will try to take advantage of the uniqueness of this Sylow subgroup and derive a generalization of Proposition 3. We note immediately that if both the Sylow $q$-subgroup and the Sylow $p$-subgroup are unique, then $G$ is abelian, and by Corollary 1 we know that the 10 DFZ inequalities (2)-(11) hold.

4.1. CASE 1: $|G| = p^2q$ AND THE SYLOW $q$-SUBGROUP IS NORMAL.

Claim 5. If $p > q$, then $G$ is in fact abelian. Hence the DFZ inequalities hold for $G$.

Proof. The Sylow $q$-subgroup is by assumption normal. It suffices to show that a Sylow $p$-subgroup is normal, for then $G$ is isomorphic to the product of its (abelian) Sylow subgroups, and hence is itself abelian. But a Sylow $p$-subgroup $G_p$ is of order $p^2$, so it has index $[G : G_p] = q$, which is the smallest prime that divides the order of $G$. It follows that $G_p$ is normal in $G$.

We could therefore assume that $p < q$, but we will state our results in full generality.

Lemma 9. Let $G$ be a group of order $p^2q$ with unique Sylow $q$-subgroup.

If $|G_{ac}|$ or $|G_{bc}|$ takes values in $\{1, p^2q, q, pq\}$, then $G_{ac}G_{bc}$ is a subgroup.

The case when $G_{ac}G_{bc}$ is not a subgroup may then only happen when ($|G_{ac}|, |G_{bc}|$) takes value in $\{(p, p), (p, p^2), (p^2, p^2)\}$. 

Proof. By Claim 5 when $p > q$ the group $G$ is abelian, hence $G_{ac}G_{bc}$ is always a subgroup.

We may therefore assume $p < q$. In order to show that $G_{ac}G_{bc}$ forms a subgroup, it suffices to show that one of $G_{ac}$, $G_{bc}$ is normal. We recall that a Sylow subgroup is unique if and only if it is normal.
We will show that any subgroup $H$ of order $1, q, pq, p^2q$ is normal. Orders $1, p^2q$ follow trivially.

Suppose $H$ has order $q$. By assumption Sylow $q$-subgroup is unique, so $H$ is the Sylow $q$-subgroup, and hence $H$ is normal. Hence $G_{ac}G_{bc}$ forms a subgroup.

Suppose $H$ has order $pq$. Then it is a subgroup of order $pq$, which has index $p$, the smallest prime that divides $|G|$. Thus it is normal. Now recall that for any two subgroups $K_1, K_2$ of $G$, the set $K_1K_2$ forms a subgroup of $G$ if either $K_1$ or $K_2$ is normal. We have so far shown that if $H$ has order $1, q, pq, p^2q$ then it is normal. Hence if either $|G_{ac}|$ or $|G_{bc}|$ takes values in $\{1, p^2q, q, pq\}$, then $G_{ac}G_{bc}$ forms a subgroup. The orders of subgroups of $G$ take value among divisors of $p^2q$, these are $\{1, p, q, p^2, pq, p^2q\}$. By removing $\{1, p^2q, q, pq\}$ from the list $\{1, p, q, p^2, pq, p^2q\}$ of possible orders for $G_{ac}$ and $G_{bc}$, we see that the only orders that might result in $G_{ac}G_{bc}$ not forming a subgroup are $\{p, p^2\}$. The second claim of the lemma now follows.

**Proposition 4.** Let $G$ be a group of order $p^2q$ with a normal Sylow $q$-subgroup $G_q$. Then any two Sylow $p$-subgroups intersect in a subgroup of order $p$.

**Proof.** It is enough to show that $G$ contains a normal subgroup of order $p$. Indeed, let $N$ be a normal subgroup of order $p$, it is contained in some Sylow $p$-group $G_p$. Let $G_p' \subset G_p$ be another Sylow $p$-subgroup, which is therefore a conjugate of $G_p$, but since the conjugate of $N$ is $N$ itself, it is contained in $G_p'$. We are left to show that $G$ contains a normal subgroup of order $p$ which is normal. Since $G_q$ is normal in $G$ we have the exact sequence

$$1 \to G_q \to G \to G_p \to 1$$

where we use $G/G_q \cong G_p$. By elementary group theory we know that $G_p$ acts on $G_q$ by conjugation. In other words, there is a homomorphism

$$\alpha : G_p \to \text{Aut}(G_q)$$

from $G_p$ to the automorphism group of $G_q$.

Case 1: If $G_p$ is cyclic of order $p^2$ then it has a unique subgroup of elements of order $p$. But that means that this subgroup is normal in $G$ because the conjugate of any element of order $p$ is another element of order $p$.

Case 2: $G_p = C_p \times C_p$.

Now $\text{Aut}(G_q) \cong C_{q-1}$ is cyclic. Hence $\alpha$ has a kernel $K \leq G_p$. But then $K$ acts trivially on $G_q$, in other words $K$ is normal in $G$.

The following proposition is analogous to Proposition 2: it examines the value $\frac{|G_{abc}|G_c|}{|G_{ac}|G_{bc}|}$, in addition classifying when this value is $\frac{2}{p}$.

**Proposition 5.** Let $G$ be a group of order $p^2q$ with a normal Sylow $q$-subgroup. Then $\frac{|G_{abc}|G_c|}{|G_{ac}|G_{bc}|} \geq 1$ and

$$\frac{|G_{abc}|G_c|}{|G_{ac}|G_{bc}|} = \frac{|G_c|}{|G_{ac}G_{bc}|} \in \{1, \frac{q}{p}, \frac{q}{p^2}, \frac{pq}{p}, pq, \frac{p^2q}{p}\}.$$

Furthermore, the case $\frac{|G_{abc}|G_c|}{|G_{ac}|G_{bc}|} = \frac{q}{p}$ occurs precisely in one of the following cases

- $|G_c| = pq$, $|G_{ac}| = |G_{bc}| = p$.
- $G_c = G$, $|G_a| = p$, $|G_b| = p^2$, and $|G_{ab}| = 1$.
- $G_c = G$, $|G_a| = p^2$, $|G_b| = p^2$ and $|G_{ab}| = p$. 

---

*Advances in Mathematics of Communications Volume 10, No. 4 (2016), 871-893*
Indeed, the restrictions on powers of $p$ cannot possibly divide $q$. Thus, the fact that $G_{ac}, G_{bc}$ are subgroups of $G_c$, we have $v_p(G_c) ≥ 1$, and to obtain $\frac{|G_{abc}|}{|G_{ac}|G_{bc}|} = q/p$ or $q/p^2$, we need $v_q(G_c) = 1$. If $|G_c| = pq$, we have

$$\frac{|G_{abc}|}{|G_{ac}||G_{bc}|} = q/p,$$

if $|G_{abc}| = 1$, \(|G_{abc}| = 1\) if $q/p = q/p^2 = q/p^2 = q$.

For the same reason as above, $G_c = G$.

If $|G_{abc}| = 1$, \(|G_{abc}| = 1\) if $q/p = q/p^2 = q/p^2 = q$.

The ratio $q/p^2$ could happen only if the intersection of two Sylow $p$-subgroups were trivial, a case that never occurs, by Proposition 4.

The next proposition is a partial generalization to groups of order $p^2q$ of Proposition 3 on groups of order $pq$. Note that reducing to the case $|G_1| = |G_2| = p$ can be used to reduce computation when looking for violators of DFZ inequalities.

**Proposition 6.** Let $G$ be a group of order $p^2q$ with normal Sylow $q$-subgroup. Let $G_1, G_2, G_3, G_4, G_5$ be arbitrary subgroups of $G$. The 10 DFZ inequalities hold for $(G, G_1, G_2, G_3, G_4, G_5)$ unless $|G_1| = |G_2| = p$.

We remark that the case $|G_1| = |G_2| = p$ remains open.

**Proof.** The case $p > q$ follows from Claim 5. We now assume $p < q$.

Recall that when either $G_1, G_2$ is normal or $G_1 = G_2$, then $G_1G_2$ is a subgroup and the DFZ inequalities hold.

By Lemma 9, we narrow down the non-normal candidates for $G_1, G_2$ to subgroups of orders $(p, p), (p, p^2), (p^2, p^2)$.

Also by Proposition 5,

$$i_{abc} = \frac{|G_{abc}|}{|G_{ac}||G_{bc}|} = \frac{|G_{c}|}{|G_{ac}|G_{bc}|} ∈ \{1, p, p^2, q, p^2q\}.$$
Evaluating $\frac{|G_{12}| |G|}{|G_1||G_2|}$ in the LHS of the 10 DFZ inequalities (2)-(11) we show that we only need to consider the case when the LHS is $\frac{q}{p}$:

- $(p, p)$ note that this case is excluded by assumption
  - if $G_1 = G_2$ then $|G_{12}| |G| = pq$
  - if $G_1 \neq G_2$ then $|G_{12}| |G| = q$

- $(p, p^2)$
  - $|G_{12}| = 1$: $|G_{12}| |G| = \frac{1}{p^3} = 2$ $\frac{q}{p}$
  - $|G_{12}| = p$: we are done since $G_1$ has order $p$, and it intersects $G_2$ in subgroup of order $p$, implying that $G_1$ is a subset of $G_2$, and inequalities hold by Corollary 1.

- $(p^2, p^2)$
  - $|G_{12}| = 1$ cannot happen since no two Sylow $p$-subgroups intersect trivially by Proposition 4.
  - $|G_{12}| = p$: $|G_{12}| |G| = \frac{p}{p^2} = \frac{q}{p}$

We have so far shown that the cases when $G_1G_2$ does not form a subgroup will have the LHS of each inequality corresponding to $\frac{q}{p}$, unless $|G_1| = |G_2| = p$.

Claim 6. Suppose that the LHS is $\frac{q}{p}$. If $v_q(RHS) \geq 1$, then the inequalities hold.

Terms on the right hand side can only take values among $\{1, p, q, pq, p^2, q^2, \frac{q}{p}\}$ by Proposition 5. The assumption $v_q(RHS) \geq 1$ means that at least one term on the RHS is taking values among $\{q, pq, q^2, \frac{q}{p}\}$. Since each of these is $\geq \frac{q}{p}$, while all other terms on the RHS are $\geq 1$, we conclude LHS $\leq$ RHS and we have proved the claim.

To complete the proof we must show that indeed $v_q(RHS) \geq 1$. This has been shown for cases of groups of order $pq$ and the proofs are identical. ☐

Let us comment on the case $(|G_1| |G_2|) = (p, p)$. Then $\frac{|G_{12}| |G|}{|G_1||G_2|} = \frac{1}{p^2} = q$ and the proof technique used above relying on $v_q(RHS) \geq 1$ is not sufficient anymore. Say $G_1, G_2$ have orders $(p, p)$ so the LHS of an inequality is $q$. But on the RHS we may have $q/p$. By Proposition 5, this will exactly happen when

- $|G_c| = pq$, $|G_{ac}| = |G_{bc}| = p$.
- $G_c = G$, $|G_a| = p$, $|G_b| = p^2$, and $|G_{ab}| = 1$.
- $G_c = G$, $|G_a| = p^2$, $|G_b| = p^2$, and $|G_{ab}| = p$.

An inequality of the form $q \leq q/p \cdot I_1 \cdot I_2 \cdot I_3$ where $q/p$ corresponds e.g. to $\frac{|G_{12}| |G|}{|G_1||G_2|}$ does not have to be true. It depends on the terms $I_1, I_2, I_3$, therefore the techniques developed in this paper do not apply immediately to this case.

Example 1. As a concrete example, consider the dihedral group $D_{20} = \langle r, s, r^{10} = s^2 = 1 \rangle$. There is one Sylow 5-subgroup, namely $r^5$. There are five Sylow 2-subgroups, given by $(s, r^5) = \{1, s, r^5, sr^5\}$ and its four conjugates, for example $r(s, r^5)r^{-1} = \{1, rsr^{-1}, r^5, rsr^4\}$. We notice the subgroup $\{1, r^5\}$ which is in the intersection of both these Sylow 2-subgroups. Take

$G_1 = \{1, rsr^{-1}\}$, $G_2 = \{1, s\}$, $G_5 = \{1, s, r^5, sr^5\}$.
Then
\[
\frac{|G_{12}| |G|}{|G_1||G_2|} = \frac{20}{4} = 5, \quad \frac{|G_{15}| |G|}{|G_1||G_5|} = \frac{20}{8} = \frac{5}{2}.
\]

4.2. Case 2: The Sylow $p$-subgroup is normal. Let us look at the other case, where the group $G$ has a normal Sylow $p$-subgroup, while the Sylow $q$-subgroup is not normal.

An analogous result as that of Lemma 5 is obtained similarly.

**Lemma 10.** Let $G$ be a group of order $p^2q$ whose Sylow $p$-subgroup is normal. Then the quantity $i_{a; b|c} \geq 1$ and
\[
i_{a; b|c} \in \{1, q, p, pq, p^2, p^2/q, \frac{p^2}{q}, q\}.
\]

**Proof.** The fact that $i_{a; b|c} \geq 1$ follows from the fact that $i_{a; b|c} = \frac{|G_{abc}| |G|}{|G_a||G_{bc}|} = \frac{|G_c|}{|G_{acG_{bc}}|}$ and $G_{acG_{bc}}$ is a subset of $G_{c}$, as before. Next
\[
\frac{|G_{abc}| |G_c|}{|G_a||G_{bc}|} = \frac{|G_c|}{|G_{acG_{bc}}|} \in q^{(-1,0,1)} p^{(0,1,2)}.
\]

The arguments is as before, the restrictions on powers of $p$ follow from Proposition 1 since the Sylow $p$-subgroup is abelian, while the restrictions on powers of $q$ come from the inclusions $G_{ac} \leq G_c$, $G_{bc} \leq G_c$ and the fact that $v_q(G_c) = 0, 1$. The case $1/q < 1$ cannot happen.

Next we look at the case when $|G| = p^2q$, $G_p$ is normal, while $G_q$ is not. If $p < q$, then, as shown below, the group is forced to be $A_4$.

**Claim 7.** Suppose $|G| = p^2q$, $G_p$ is normal, while $G_q$ is not, and $p < q$. Then $G \cong A_4$. Hence 10 DFZ inequalities hold for $G$.

**Proof.** Since $G_p$ is normal and $G_q \cong C_q$, we have an exact sequence
\[
1 \to G_p \to G \to C_q \to 1
\]
and $C_q$ acts on $G_p$, i.e. there is a homomorphism
\[
\alpha : C_q \to \text{Aut}(G_p)
\]
Note that the assumption that $G_q$ is not normal implies that $G$ cannot be abelian. This means that the action induced by $\alpha$ is nontrivial.

There are two cases to consider:

- If $G_p = C_{p^2}$, then $G$ would in fact be forced to be abelian:
  We recall that the automorphism group $\text{Aut}(C_{p^2}) \cong \mathbb{Z}_{p^2} \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_p$ has order $(p-1)p$. Hence the image of any homomorphism $\alpha : C_q \to \text{Aut}(G_p)$ divides $p-1$. But it must also divide $|C_q| = q$. Since by assumption $p < q$, we conclude that the image of $\alpha$ is $\{1\}$, i.e., $\alpha$ is trivial. In other words $\alpha$ induces trivial action of $G_q$ on $G_p$. This makes $G$ an abelian group, contradicting the assumption that $G_q$ is not normal.

- If $G_p = C_p \times C_p$, we know that $\text{Aut}(G_p)$ is the general linear group $GL_2(\mathbb{F}_p)$ of order $(p^2-1)(p-2)$. We consider the case when the image of $\alpha$ is nontrivial, so is of order $q$. For $q$ to divide $(p^2-1)(p^2-p)$, together with the assumption $p < q$, we would need that $q \mid p+1$ and so $p = 2$ and $q = 3$. Therefore $G$ is a nonabelian semidirect product of $C_2 \times C_2$ and $C_3$. Up to isomorphism the only such group is $A_4$, as claimed.
We have completed showing the claim. It can be checked numerically that $A_4$ does not violate any of the $10$ DFZ inequalities.

Therefore we may assume that $q < p$. Here is the analogue of Lemma 9.

**Lemma 11.** Let $G$ be a group of order $p^2q$ with normal Sylow $p$-subgroup. Assume that $q < p$.

If $|G_{ac}|$ or $|G_{bc}|$ takes values in $\{1, p^2q, p, p^2\}$, then $G_{ac}G_{bc}$ is a subgroup. The case when the set $G_{ac}G_{bc}$ is not a subgroup happens only when the orders $(|G_{ac}|, |G_{bc}|)$ take values in $\{(q,q),(q,pq),(pq,pq)\}$.

**Proof.** It suffices to show that any subgroup $H$ of order $1, p^2q, p, p^2$ is normal.

Orders $1,p^2$ follow trivially. For order $p$, it follows from the uniqueness of the Sylow $p$-subgroup. For $p^2$, this is because a subgroup of order $p^2$ has index $q$, the smallest prime that divides $|G|$, thus it is normal. The second claim follows from removing $\{1, p^2q, p, p^2\}$ from the list $\{1, q, p, p^2, pq, p^2q\}$ of possible orders.

Therefore, we may conclude as in Proposition 6.

**Proposition 7.** Let $G$ be a group of order $p^2q$ with normal Sylow $p$-subgroup. Let $G_1, G_2, G_3, G_4, G_5$ be arbitrary subgroups of $G$. The $10$ DFZ inequalities hold for $(G,G_1,G_2,G_3,G_4,G_5)$ unless $|G_1| = |G_2| = q$.

**Proof.** The case $p < q$ is taken care of by Claim 7. The proof for the case $q < p$, where we now apply Lemma 11 instead of Lemma 9 is similar as in Proposition 6. As a result of Lemma 11, the only non-normal candidates for $G_1, G_2$ will give as possible values for $(|G_1|, |G_2|)$ the pairs $(q,q), (q,pq), (pq,pq)$.

Examining the possibilities for the LHS of equations (2)-(11) gives

- $(q,q)$ note that this case is dropped by assumption
  
  if $G_1 \neq G_2$ then $\frac{|G_{12}||G|}{|G_1||G_2|} = \frac{1}{q^2} = p^2/q$
  
  if $G_1 = G_2$ then $\frac{|G_{12}||G|}{|G_1||G_2|} = \frac{q}{p^2q} = p^2$.

- $(q,pq)$
  
  if $|G_{12}| = 1$, then $\frac{|G_{12}||G|}{|G_1||G_2|} = \frac{1}{q} = p/q$
  
  if $|G_{12}| = q$, since $G_1$ has order $q$, and it intersects $G_2$ in a subgroup of order $q$, $G_1$ is a subset of $G_2$, and inequalities hold by Corollary 1.

- $(pq,pq)$
  
  if $|G_{12}| = 1$ then $\frac{|G_{12}||G|}{|G_1||G_2|} = \frac{1}{q} = p/q$ which is not possible
  
  if $|G_{12}| = q$ then $\frac{|G_{12}||G|}{|G_1||G_2|} = \frac{q}{pq} = 1$, and inequalities hold as RHS $\geq 1$
  
  if $|G_{12}| = p$ then $\frac{|G_{12}||G|}{|G_1||G_2|} = \frac{p}{pq} = p/q$.

We observe that the cases for which it remains to establish the inequality have $v_p(LHS) \geq 1$. We proceed with the proof as in Proposition 5, only now we use valuation $v_p$ at $p$ in an analogue of Claim 6.

---

5. **Group violations**

5.1. **Violations by $S_4$.** We prove that the symmetric group $S_4$ violates two of the ten DFZ inequalities, and so does the projective group $PGL_2(\mathbb{F}_q)$, for $q$ a prime power.
Proposition 8. The symmetric group $S_4$ of permutations on 4 elements violates (2) and (4).

Proof. Consider $G = S_4$. Rewrite the inequality (2) in its group form:

(12) \[ GI(X_1; X_2) \leq GI(X_1; X_2|X_3)GI(X_1; X_2|X_4)GI(X_3; X_4|X_5)GI(X_1; X_5) \]

which simplifies to

\[ |G_{12}||G_{13}||G_{23}||G_{14}||G_{24}||G_{35}||G_{45}| \leq |G_2||G_3||G_{123}||G_{15}||G_{124}||G_4||G_{345}|. \]

Take

\[ G_1 = \langle (3, 4), (2, 4, 3) \rangle, \quad G_3 = \langle (1, 2)(3, 4), (3, 4) \rangle \]
\[ G_2 = \langle (1, 3), (1, 3, 2) \rangle, \quad G_4 = \langle (1, 3)(2, 4), (2, 4) \rangle \]
\[ G_5 = \langle (1, 4)(2, 3), (1, 3)(2, 4) \rangle \]

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

\[ G_1 \cap G_2 = \langle (2, 3) \rangle, \quad G_1 \cap G_3 = \langle (3, 4) \rangle \]
\[ G_2 \cap G_3 = \langle (1, 2) \rangle, \quad G_1 \cap G_4 = \langle (2, 4) \rangle \]
\[ G_2 \cap G_4 = \langle (1, 3) \rangle, \quad G_1 \cap G_5 = \{1\} \]
\[ G_4 \cap G_5 = \langle (1, 3)(2, 4) \rangle, \quad G_3 \cap G_4 \cap G_5 = \{1\} \]
\[ G_3 \cap G_5 = \langle (1, 2)(3, 4) \rangle, \quad G_1 \cap G_2 \cap G_3 = \{1\} \]

But for the trivial group, all the other intersection subgroups are of order 2. The left hand side of (12) yields

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

while the right hand side is

\[ |G_2||G_3||G_{123}||G_{15}||G_{124}||G_4||G_{345}| = 6 \cdot 4 \cdot 1 \cdot 1 \cdot 4 \cdot 1 = 96. \]

Next, rewrite the inequality (4) in its group form

\[ GI(X_1; X_2) \leq GI(X_1; X_3)GI(X_1; X_2|X_4)GI(X_2; X_5|X_3)GI(X_1; X_4|X_3, X_5) \]

which becomes

(13) \[ |G_{12}||G_{14}||G_{24}||G_{23}||G_{135}||G_{345}| \leq |G_2||G_3||G_{124}||G_4||G_{253}||G_{1345}|. \]

Take

- $G_1 = \langle (3, 4), (2, 4, 3) \rangle$, $|G_1| = 6$,
- $G_2 = \langle (1, 2)(3, 4), (3, 4) \rangle$, $|G_2| = 4$,
- $G_3 = \langle (1, 2)(3, 4), (1, 4)(2, 3), (1, 3) \rangle$, $|G_3| = 8$,
- $G_4 = \langle (1, 3), (1, 3, 2) \rangle$, $|G_4| = 6$,
- $G_5 = \langle (1, 3)(2, 4), (2, 4) \rangle$, $|G_5| = 4$.

so that

\[ G_{12} = \langle (3, 4) \rangle, \quad G_{14} = \langle (2, 3) \rangle, \quad G_{13} = \langle (2, 4) \rangle, \]
\[ G_{24} = \langle (1, 2) \rangle, \quad G_{23} = \langle (1, 2)(3, 4) \rangle , \]
\[ G_{135} = \langle (2, 4) \rangle, \quad G_{345} = \langle (1, 3) \rangle \]

and the left hand side of (13)

\[ |G_{12}||G_{14}||G_{24}||G_{23}||G_{135}||G_{345}| = 2 \cdot 2 \cdot 2 \cdot 2 = 64 \]

which is strictly larger than

\[ |G_2||G_3||G_{124}||G_4||G_{253}||G_{1345}| = 4 \cdot 2 \cdot 1 \cdot 6 \cdot 1 \cdot 4 = 48. \]
Let \( GL_2(\mathbb{F}_p) \) be the general linear group of order 2 over \( \mathbb{F}_p \). It has order \((p^2 - 1)(p^2 - p)\), and naturally acts on the projective line \( \mathbb{P}(\mathbb{F}_p) \), whose \( p + 1 \) elements can be written (in homogeneous coordinates) as \{(0, 1), (1, 1), \ldots, (p-1, 1), (1, 0)\}. This action descends to a faithful action of \( PGL_2(\mathbb{F}_p) \), the projective general linear group over \( \mathbb{F}_p \), of degree 2, on \( \mathbb{P}(\mathbb{F}_p) \), which permutes the elements of \( \mathbb{P}(\mathbb{F}_p) \). This thus yields an injective homomorphism from \( PGL_2(\mathbb{F}_p) \) to the symmetric group \( S_{p+1} \). For \( p = 3 \), \(|PGL_2(\mathbb{F}_3)| = 24 = |S_4|\), showing that \( PGL_2(\mathbb{F}_p) \cong S_4 \).

This suggests to look at the group \( PGL_2(\mathbb{F}_q) \), \( q \) a prime power, to find examples of violators. Indeed, it is exactly known when \( S_4 \) is contained in \( PGL_2(K) \), for \( K \) an arbitrary field.

**Proposition 9** ([13, 2.5]). Suppose that the characteristic of \( K \) is prime to the order of \( S_4 \). Then \( PGL_2(K) \) contains \( S_4 \) if and only if \(-1\) is a sum of two squares in \( K \).

It follows that whenever \( p \geq 5 \), then \( PGL_2(\mathbb{F}_q) \) contains \( S_4 \), for \( q = p^r \), for \( r \geq 1 \). The proof of the following result is attributed to Henry Mann [8] (the result holds for characteristic 2, with a different proof).

**Proposition 10.** Suppose that the characteristic of \( \mathbb{F}_q \) is not 2. Every element of \( \mathbb{F}_q^* \) is a sum of two squares.

**Proof.** Consider the map \( \phi \), which maps \( x \) to \( x^2 \). Suppose \( \phi(a) = \phi(b) \), then \( a^2 = b^2 \iff (a - b)(a + b) = 0 \iff a = b \) or \( a = -b \). Therefore \( \phi \) restricted to \( \mathbb{F}_q^* \) sends two distinct elements of \( \mathbb{F}_q^* \) to a single element, from which we deduce that exactly half of the elements of \( \mathbb{F}_q^* \) are squares. Since 0 is also a square, the set \( S \) of squares in \( \mathbb{F}_q \) contains \((q + 1)/2 \) elements.

Next, we look at the additive structure of \( \mathbb{F}_q \), and pick \( a \in \mathbb{F}_q \). Notice that \(|S| = |a - S| = |\{a - s, s \in S\}|\). Since \(|S| + |a - S| > |\mathbb{F}_q|\), \(|S| \cap |a - S|\) is not empty. Take \( s' = a - s \) in the intersection, then \( a = s' + s \), and is therefore a sum of two squares.

Therefore another example of group violating the inequalities (2) and (4) after \( S_4 \) is \( PGL_2(\mathbb{F}_5) \) of order 120, which turns out to be isomorphic to \( S_5 \) (the same proof as above holds).

### 5.2. Smallest Violators

From Corollary 1, abelian groups never violate the 10 DFZ inequalities. From Proposition 3, neither do groups of order \( pq \) for \( p, q \) two distinct primes. Thus until order 23 (included), only 8, 12, 16, 18, and 20 are orders where potential violators could exist. Suppose there exists an abelian group \( A \) such that for every choice of subgroups \( G_1, \ldots, G_n \) of \( G \), there exist subgroups \( A_1, \ldots, A_n \) of \( A \) such that \(|G : G_i| = |A : A_i|\) for every non-empty subset \( A \) of \( \{1, \ldots, n\} \), and \( G_A = \cap_{i \in A} G_i \), \( A_A = \cap_{i \in A} A_i \). Then we say that \( G \) is abelian group representable. Groups of order 8 are known to be abelian group representable [14] and can be ruled out as well. Groups of orders 12, 16, 18, 20 are left, apart 16, all of them fit in the category of groups of order \( p^2q \). However, since the case of \(|G_1| = |G_2| = p \) is still incomplete, we checked numerically that no violation of the 10 DFZ inequalities is to be found. Therefore the smallest violator is of order 24.

### 5.3. Simultaneous Violators

One may wonder whether it is possible to find a simultaneous group violator for the ten DFZ inequalities. We provide a negative answer.
Definition 1. If a finite group $G$ and subgroups $G_1, \ldots, G_n$ violate two or more inequalities, then $(G, G_1, \ldots, G_n)$ is called a simultaneous group violator for those inequalities.

Proposition 11. There do not exist any simultaneous group violators for (2) and (4).

Proof. Suppose $(G, G_1, G_2, G_3, G_4, G_5)$ are a simultaneous group violator of the group inequalities of (2) and (4). That is,

$$|G_{12}| |G_{13}| |G_{23}| |G_{14}| |G_{24}| |G_{35}| |G_{45}| > |G_2| |G_3||G_{123}| |G_{15}| |G_{124}| |G_4||G_{345}|$$

and

$$|G_{12}| |G_{14}| |G_{24}| |G_{23}| |G_{135}| |G_{345}| > |G_2| |G_{13}| |G_{124}| |G_4||G_{235}| |G_{1345}|.$$

Since all these quantities are positive the product of the inequalities yields:

$$|G_{12}|^2 |G_{23}|^2 |G_{14}|^2 |G_{24}|^2 |G_{35}| |G_{45}| |G_{135}| > |G_2|^2 |G_{123}| |G_3||G_{14}|^2 |G_{24}|^2 |G_{35}| |G_{135}| \tag{14}$$

But using the Lemma 3 repeatedly (its application indicated by parentheses), we have

$$|G_{12}|^2 |G_{23}|^2 |G_{14}|^2 |G_{24}|^2 |G_{35}| |G_{45}| |G_{135}| \leq |G_2|^2 |G_{123}| |G_2||G_{124}| |G_{23}| |G_{14}|^2 |G_{24}| |G_{35}| |G_{135}|$$

$$\leq |G_2|^2 |G_{123}| |G_3||G_{235}| |G_4||G_{14}|^2 |G_{124}| |G_{35}| |G_{135}|$$

$$\leq |G_2|^2 |G_{123}| |G_3||G_{235}| |G_4||G_{124}|^2 |G_{145}| |G_{135}|$$

$$\leq |G_2|^2 |G_{123}| |G_3||G_{145}| |G_4||G_{124}|^2 |G_{235}| |G_{1345}|,$$

a contradiction to inequality (14) which concludes the proof. \hfill \square

Corollary 4. There do not exist any simultaneous group violators for all DFZ inequalities.

Proof. If there exists a simultaneous group violator for all DFZ inequalities, it violates (2) and (4) simultaneously, a contradiction to Proposition 11. \hfill \square

References

[1] T. H. Chan and R. W. Yeung, On a relation between information inequalities and group theory, IEEE Trans. Inform. Theory, 48 (2002), 1992–1995.
[2] R. Dougherty, C. Freiling and K. Zeger, Linear rank inequalities on five or more variables, preprint, arXiv:0910.0284
[3] D. S. Dummit and R. M. Foote, Abstract Algebra, Hoboken, Wiley, 2004.
[4] C. F. Gardiner, A First Course in Group Theory, Springer, 2013.
[5] D. Hamer, A. Romanenko, A. Shen and N. Vereshchagin, Inequalities for Shannon entropy and Kolmogorov complexity, in Proc. 12th Ann. IEEE Conf. Comp. Comp., IEEE, 1997, 13–23.
[6] B. Hassibi and S. Shadbakht, Normalized entropy vectors, network information theory and convex optimization, in 2007 Inform. Theory Workshop (ITW 2007), 2007.
[7] A. Ingleton, Representation of matroids, Combin. Math. Appl., (1971), 23.
[8] H. Mann, Additive group theory — a progress report, Bull. Amer. Math. Soc., 79 (1973), 1069–1075.
[9] W. Mao and B. Hassibi, Violating the Ingleton inequality with finite groups, in 47th Ann. Allerton Conf. Commun. Contr., IEEE, 2009, 1053–1060.
[10] N. Markin, E. Thomas and F. Oggier, Groups and information inequalities in 5 variables, in Allerton'14 Proc. 52nd Ann. Allerton Conf. Commun. Control Comp., IEEE, 2013, 804–809.
[11] F. Matés, Conditional independences among four random variables I, *Combin. Prob. Comp.*, 4 (1995), 269–278.

[12] J. J. Rotman, *An Introduction to the Theory of Groups*, Springer, 1999.

[13] J.-P. Serre, Propriétés galoisiennes des points d’ordre fini des courbes elliptiques, *Invent. Math.*, 15 (1971), 259–331.

[14] E. K. Thomas, N. Markin and F. Oggier, On Abelian Group Representability of Finite Groups, *Adv. Math. Commun.*, 8 (2014), 139–152.

[15] X. Yan, R. Yeung and Z. Zhang, The capacity for multi-source multi-sink network coding, in *2007 Int. Symp. Inform. Theory (ISIT 2007)*, Nice, 2007.

Received March 2015; revised August 2015.

*E-mail address:* nadyaomarkin@gmail.com

*E-mail address:* ELDHO1@e.ntu.edu.sg

*E-mail address:* frederique@ntu.edu.sg